Opinnäytetyö (AMK)

Tietojenkäsittely

Tietoliikenne

2010

Lassi Murto & Matti Sipola

RFID/NFC -TEKNIIKAN VAIKUTUS KULUTTAJIIN

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

Turun ammattikorkeakoulu

Tietojekäsittely | Tietoliikenne

Marraskuu 2010 | 77

Ohjaaja Esko Vainikka

Lassi Murto & Matti Sipola

RFID/NFC -TEKNIIKAN VAIKUTUS KULUTTAJIIN

Opinnäytetyössä on kartoitettu RFID/NFC-etätunnistustekniikan sovellusten käyttöä kotitalouksissa. Työn tarkoituksena on kartoittaa tekniikan tämänhetkistä tilannetta niin Suomessa kuin ulkomaillakin sekä pohtia etätunnistustekniikan tulevaisuutta kotitalousympäristössä.

Opinnäyte tehtiin toimeksiantona Turun ammattikorkeakoululle. Ajatus opinnäytteen aiheesta syntyi projektityökurssin aikana, jolloin perehdyttiin ensimmäistä kertaa RFID-tekniikkaan ja sen käytännön sovelluksiin. Työssä käsitellään RFID/NFC-tekniikan peruskäsitteet, joiden avulla pyritään luomaan eheä kokonaiskuva järjestelmän toiminnasta. Tietoturvaosiossa perehdytään aiheen keskeisimpiin uhkakuviin ja niiden hallintaan.

Tutkimustyön perusteella voidaan todeta, että ihmiset ovat tietämättään käyttäneet tekniikkaa jo kauan. Erilaiset kuluvalvontasovellukset ja autojen keskuslukituksen kaukosäätimet ovat jo pitkään toimineet lyhyen kantaman RFID-tekniikalla. Logistiikassa ollaan siirtymässä yhä enemmän RFID-tekniikalla toimivaan toimitusketjujen hallintaan. Käytännössä tämä näkyy kotitalouksissa mahdollisuutena seurata esimerkiksi pakettien liikkumista postin jakelujärjestelmissä.

ASIASANAT:

RFID, radio frequency identification, RFID-tunnistus, NFC, tietoturva, etätunnistaminen, mobiilimaksaminen, kaupunkikortti

BACHELOR´S THESIS | ABSTRACT
TURKU UNIVERSITY OF APPLIED SCIENCES

Data processing | Data communication

November 2010 | 77

Instructor Esko Vainikka

Lassi Murto & Matti Sipola

THE INFLUENCE OF RFID/NFC-TECHNOLOGY ON CONSUMERS

For this thesis the use of RFID and NFC technology applications in households were surveyed. The objective of this work was to survey the current use of technology in Finland as well as abroad, not forgetting the future of identification technology in the household environment.

The thesis was completed as an assignment for Turku University of Applied Sciences. The idea for the thesis originated from a course project where we familiarized ourselves for the first time with RFID technology and its applications. In our work we discuss the basic concepts of RFID and NFC technologies, through which we tried to produce a sound understanding of how the system operates. In the information security section we wanted to concentrate on the central threats surrounding the subject and how to manage them.

Based on our research it can be said that we have been using this technology for years without realizing it. Different access control applications and remote controls for cars' central locking system have been using short range RFID technology more and more for a long time before now. In logistics there is a move towards utilising RFID technology in controlling supply chains. In practice this can be seen in households for example as a possibility to follow the movements of parcels in the post office's delivery system.

KEYWORDS:

RFID radio frequency identification, NFC, near field communication, contactless card, information security. mobile payment

SISÄLTÖ

LIITTEET

KUVAT

KUVIOT

TAULUKOT

KÄYTETYT LYHENTEET

BAP	Battery Assisted Passive, semipassiivinen eli paristoavusteinen RFID-tunniste.
BVG	Berliner Verkehrsbetriebe, Berliinin julkisenliikenteen yritys.
EAN	European Article Numbering, viivakoodi.
EEPROM	Electrically Erasable Programmable Read Only Memory, uudelleenohjelmoitava muistityyppi.
EHF	Extremely High Frequency, radiotaajuusalue välillä 30 - 300 GHz.
EPC	Electronic Product Code, sähköinen tuotekoodi.
ERP	Enterprise Resource Planning, yritysten toiminnanohjausjärjestelmä.
ETSI	European Telecommunication Institute, Eurooppalainen voittoa tavoittelematon standardointielin.
Eur-Lex	Euroopan unionin oikeus.
FCC	Federal Communications Commission, Yhdysvaltojen hallituksen alainen telekommunikaatiovirasto.
FeliCa	Felicity Card, Sonyn kehittämä kontaktiton RFID-älykortti.
Finlex	Suomen oikeusministeriön ylläpitämä oikeudellinen tietokanta.
GSM	Global System for Mobile Communications, maailmanlaajuisesti toimiva matkapuhelinverkko.
HF	High Frequency, taajuusalue 3 - 30MHz:n välillä.
IEC	International Electrotechnical Commission, kansainvälinen voittoa tavoittelematon sähköalan standardointiorganisaatio.
IrDa	Langattomaan tiedonsiirtoon käytettävä tekniikka, joka toimii infrapuna-aalloilla.
ISM	Industrial, Scientific and Medical on maailmanlaajuinen radiotaajuuskaista, jonka käyttö ei vaadi erillistä lupaa ja on alun perin tarkoitettu teolliseen, tieteelliseen ja lääketieteelliseen käyttöön.
ISO	International Organization for Standardization, maailman yleisin standardointielin.
LF	Low Frequency on 30kHz - 300kHz välillä toimiva radioaaltotaajuus.

MTS	Mobile TeleSystems, Venäjän suurin teleoperaattori.
NFC	Near Field Communication on lyhyen kantaman korkeataajuinen langaton tiedonsiirto-tekniikka, joka mahdollistaa datasiirron kahden elektronisen laitteen välillä.
OV-chipkaart	Openbaar vervoer chipkaart, hollantilainen julkisenliikenteen älykortti.
PIN	Personal Identification Number, tunnusluku tai salasana, joka vastaa toiminnaltaan allekirjoitusta.
RFID	Radio Frequency Identification on radiotaajuuksilla toimiva etätunnistustekniikka.
S-Bahn	Stadtschnellbahn, Itävallassa, Saksassa ja Sveitsissä toimiva metroverkosto.
SAP	Saksalainen toiminnanohjausjärjestelmiä valmistava yritys.
SHF	Super High Frequency, mikroaaltojen taajuusalue välillä 3 - 30GHz.
SKU	Stock Keeping Unit kertoo mihin tuoteryhmään joku artikkeli kuuluu.
VRR	Verkehrsverbund Rhein-Ruhr, saksalainen joukkoliikenneyhdistys, joka palvelee alueella Rhein-Ruhr.
VRS	Verkehrsverbund Rhein-Sieg, saksalainen joukkoliikenneyhdistys, joka palvelee alueella Rhein-Sieg.
WORM	Write Once Read Many, kerran ohjelmoitava monta kertaa luettavissa oleva muistityyppi.
U-Bahn	Untergrundbahn, saksalainen metroverkosto.
UHF	Ultra High Frequency, taajuusalue 300MHz - 3GHz.

1 JOHDANTO

Opinnäytetyön tarkoituksena on luoda eheä kokonaiskuva RFID/NFC-tekniikasta, sekä sen perusteista että myös käytännön sovellusmaailmasta Suomessa ja ulkomailla. Tarkoituksena on myös kartoittaa tämän hetken tilannetta tekniikan hyödyntämisestä kuluttajiin vaikuttavissa sovelluksissa sekä luoda realistinen visio tulevaisuuden näkymistä.

Kyseessä on kuuma aihe, koska tutkimamme tekniikka on nyt murrosvaiheessa ja todellisen läpimurron uskotaan tapahtuvan lähiaikoina. Tekniikka tulee vaikuttamaan kaikkien elämään kaikilla aloilla yleisestä mielipiteestä riippumatta. Aihe on valittu, koska RFID ja NFC eivät aikaisemmin olleet tuttuja, vaan vasta keväällä 2010 saimme paneutua aiheen pariin koulun tarjoamalla projektityökurssilla.

Olemme valinneet näkökulmaksi kuluttajat ja tutkimme, miten tekniikat ovat jo osana heidän elämäänsä, sekä miten tekniikat tulevat mullistamaan tulevaa arkea. Lähestymistapana on käytetty evaluoivaa ja vertailevaa tutkimusta. Kartoitamme eri alueiden tilannetta liittyen tutkimaamme tekniikkaan sekä pohdimme alueellisia eroja.

Tärkeimpinä löydöksinä voidaan pitää muun muassa sitä, että tekniikka ei ole niin uusi, kuin alussa kuviteltiin. Lisäksi kuluttajanäkökulmasta katsoen NFC on RFID:tä paljon tärkeämpi ja NFC-tekniikan kohdalla Suomi nousi yllättäen yhdeksi tärkeimmistä kehittäjämaista. Yllätyksenä tulivat myös alueelliset erot kokemuksissa sekä Euroopan heikko asema verrattuna Amerikkaan ja Aasiaan.

Tutkimuksemme teoreettinen viitekehys koostuu tekniikan perusteista, alan standardeista ja lainsäädännöstä. Empiirisessä osassa paneudutaan tekniikan käyttöön, niin nykyään kuin tulevaisuudessa.

2 RFID – RADIO FREQUENCY IDENTIFICATION

RFID (Radio Frequency Identification) on radioaalloilla tapahtuvaa tiedonsiirtoa, joka mahdollistaa esineiden ja ihmisten yksilöllisen tunnistuksen. Tekniikkaa verrataan usein viivakoodiin (barcode; EAN), mutta toisin kuin viivakoodin lukeminen, RFID-tunnistus voi tapahtua ilman näköyhteyttä. RFID-tunniste sisältää EPC-koodin (Electronic Product Code), joka linkitetään taustajärjestelmässä olevaan tietokantaan. Esimerkiksi elektroniseen RFID-avaimeen voidaan myöhemmin lisätä tai poistaa siitä oikeuksia. Perinteistä viivakoodia on mahdotonta muuttaa jälkikäteen. Kohteeseen kiinnitetään tunniste, jonka avulla taustajärjestelmän tietokannasta voidaan hakea kohteesta tietoja. (Hunt ym. 2007, 1.)

Historia

Menetelmän historia sijoittuu II maailmansodan aikaiseen tutkan kehittymiseen. Sir Robert Alexander Watson-Watt kehitti jo olemassa olevaa tutkaa vuonna 1935 ja sen ansiosta sodassa voitiin varoittaa lähestyvistä vihollisten lentokoneista. Sodan aikana britit kehittivät niin sanotun identify friend or foe -tunnistusjärjestelmän, joka on maailman ensimmäinen RFID-järjestelmä. Neuvostoliitto sovelsi tekniikkaa vakoilukäytössä vuodesta 1945 lähtien. (Seppä 2009, 12.)

Kunnian ensimmäisestä RFID-tekniikkaa muistuttavan laitteen patentista sai vuonna 1973 Mario Cardullo. Hän loi passiivisen RFID-tunnisteen (passive tag), jossa oli pieni muistipiiri. Ensimmäinen patentti, jonka hakemuksessa mainittiin RFID-lyhenne, hyväksyttiin Charles Waltonille vasta vuonna 1983. (RFID Journal 2010.)

Vasta 1980-luvulla ensimmäiset kaupalliset RFID-järjestelmät, kuten tietullit, tulivat yksityishenkilöiden saataville. Yhdysvalloissa tekniikan soveltamisen pääpaino oli tuolloin erilaisten logistiikkasovellusten ja kulunvalvontajärjestelmien kehittämisessä. Euroopassa mielenkiinnon kohteena oli tunnistaa kotieläimiä RFID-tekniikkaa hyödyntäen sekä kartoittaa

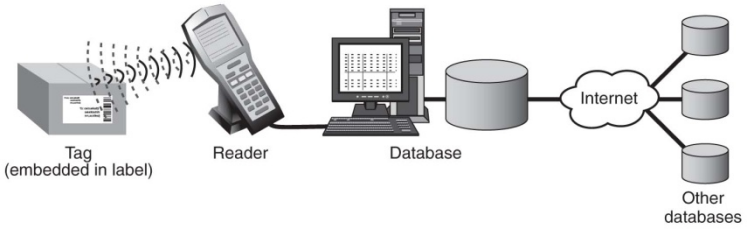
mahdollisuuksia käyttää tekniikkaa myös teollisuudessa. 1980-luvulla otettiin käyttöön ensimmäiset RFID-tekniikalla toimivat hiihtokeskuksien hissilippusovellukset. Tekniikan kehityttyä 1990-luvulla Yhdysvalloissa käytössä olleet tietullisovellukset kehittyivät niin, että ne voitiin ottaa käyttöön moottoritienopeuksilla. Kiinnostus tekniikkaa kohtaan on kasvanut 2000-luvulla entisestään. Uusia sovellusalueita kehitellään jatkuvasti. Tulevaisuudessa on mahdollisuus käyttää RFID-tekniikkaan pohjautuvaa NFC-tekniikkaa erilaisten hyödykkeiden maksamisessa. (Kärkkäinen 2006.)

2.1 Järjestelmäkokonaisuus

Toimiva RFID-järjestelmä koostuu tuotteisiin kiinnitettävästä tunnisteesta (tag), RFID-lukijasta (reader) ja tietokantaan yhteydessä olevasta taustajärjestelmästä (back end) (Hunt ym. 2007, 5). Järjestelmän käyttö vaatii ammattitaitoisen ja koulutetun käyttäjäkunnan. Yksinkertaistettuna RFID-järjestelmän ideana on, että lukija ja tunniste kommunikoivat keskenään ilmateitse samalla taajuudella.

Monissa eri tietolähteissä on väitetty RFID-järjestelmän syrjäyttävän perinteisen, pitkään käytössä olleen EAN-viivakoodijärjestelmän piakkoin. Väite on mielestämme turhan optimistinen, koska RFID-järjestelmät ovat vielä hyvin kalliita toteuttaa, johtuen siitä, että järjestelmien myyntivolyymit ovat vielä niin pieniä. Selvää on kuitenkin se, että RFID-järjestelmiä otetaan EAN-järjestelmien rinnalle asteittain.

RFID-tunnisteen tiedot siirtyvät kuvan 1 mukaisesti lukijan kautta väliohjelmistoon ja yhä eteenpäin taustajärjestelmässä sijaitsevaan tietokantaan. (United States Government Accountability Office 2009, 5.)

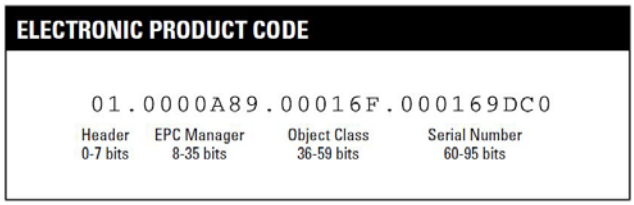


Kuva 1. RFID-järjestelmäkokonaisuus (United States Government Accountability Office 2005, 5).

2.1.1 Tunnisteet

RFID-tunniste eli tagi koostuu pääosin kahdesta komponentista, sirusta tai integroidusta piiristä ja antennista. (Hunt ym. 2007, 6.) Lisäksi tunniste voi sisältää oman virtalähteen. Tunnisteet voivat olla erikokoisia ja -muotoisia. Tunnisteiden ulkonäkövalintoihin vaikuttavat niiden käyttökohteet. Pienimmät tunnisteet ovat kooltaan 0,4 mm x 0,4 mm ja niiden lukuetäisyys on vain muutama senttimetri. (ZEBRA Technologies 2010.) Tunniste kiinnitetään tunnistettavaan kohteeseen. Valmistusvaiheessa jokainen tunniste on merkitty yksilöllisellä sarjanumerolla, eli EPC-koodilla (Electronic Product Code). Lisäksi tunniste voidaan sulkea hermeettisen eli ilmatiiviin kuoren sisään, jolloin tunnisteen siruun ei enää päästä käsiksi. EPC-koodi eli sähköinen tuotekoodi on 64- tai 96-bittinen koodi, joka on tallennettu sähköisesti RFID-tunnisteeseen. Koodi on jaettu numerosarjoihin, joiden avulla saadaan lisätietoa tuotteesta. (Sweeney II 2005, 38.)

Kuvan 2 ensimmäinen lohko (header) määrittää EPC-koodin rakenteen, joka sisältää koodin tyyppitiedot, rakenteen, version sekä käytettävän EPC-sukupolven. Toinen lohko (EPC-manager) sisältää tiedot tunnistettavan kohteen valmistajasta. Kolmas lohko (Object class) sisältää kohteen tuotetunnuksen (SKU), jonka avulla kohde paikannetaan lähettäjän varastosta. Viimeinen lohko (serial number) kertoo tunnisteen sarjanumeron, joka on samalla tuotteen sarjanumero. (Sweeney II 2005, 47.)



Kuva 2. EPC-koodin rakenne (Sweeney II 2005, 46).

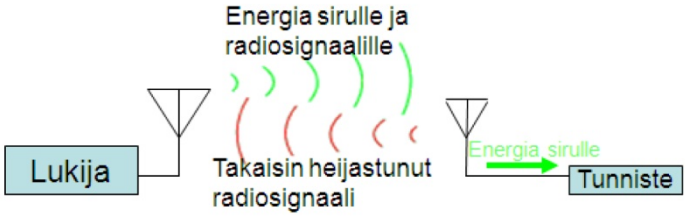
Tunnisteelle voidaan kirjoittaa tietoa, mutta yleensä tunniste sisältää vain EPC-koodin, jolla haetaan tiedot taustajärjestelmästä. RFID-tunnisteet voivat olla passiivisia, semi-passiivisia, aktiivitunnisteita ja SAW-tunnisteita. (Sweeney II 2005, 38.)

Passiivitunnisteet

Passiiviset tunnisteet jaetaan kahteen eri ryhmään jännitteen- ja tiedonsyöttötekniikan mukaisesti: matalan (LF) ja korkean taajuuden (HF) tunnisteet käyttävät sähkömagneettista induktiota. Korkeampien taajuuksien tunnisteet (VHF, UHF ja SHF) käyttävät sähkökentän heijastumista (backscatter) tiedon ja käyttöjännitteen siirtämiseen kuvan 3 esittämällä tavalla. VHF- ja SHF-taajuudet eivät ole käytössä RFID-järjestelmissä. (TOP Tunniste 2006.) Passiivitunnisteiden hintojen keskiarvo vaihtelee 0,09 € – 0,11 € hankintavolyymien mukaan. Viimeisen vuoden sisällä hinnat ovat laskeneet pienimmissä volyymeissa (~10000 kpl) noin 1,5 %, kun taas suuremmissa määrissä (~100000 kpl) ne ovat pysyneet ennallaan. (Odin 2010b.)

Passiivinen RFID-tunniste ei sisällä omaa virtalähdettä, ja koska se ei ole riippuvainen paristosta, sen elinikä on pitkä. Tunnisteen rakenne antaa näin

ollen sen käyttöympäristöille lukuisia mahdollisuuksia. Tunnisteen voi esimerkiksi sijoittaa eläimen ihon alle tunnistamista varten. Uusissa Europasseissa on sisäänrakennettu RFID-passiivitunniste, joka tekee passien väärentämisestä lähes mahdotonta. RFID-lukija yhdessä antenninsa kanssa muodostavat ympärilleen sähkömagneettisen kentän, josta tunniste vastaanottaa energiansa (Finkenzeller 2003, 13). Koska tunniste saa virtansa lukijalta, on signaalin oltava erittäin vahva ja näin ollen etäisyyden lukijan ja tunnisteen välillä on oltava lyhyt. Toisaalta lyhyt lukuetäisyys tekee tunnisteen tietoturvalliseksi. (Kranenburg & Ward 2006, 9.) Passiiviset tunnisteet ovat yksinkertaisen rakenteen ja pienen kokonsa ansiosta edullisimpia valmistaa, mistä syystä ne ovat maailmalla hyvin suosittuja. Kappalehinta vaihtelee tilattavien tunnisteiden määrän mukaan kolmesta sentistä ylöspäin. Passiivitunnisteet ovat näin ollen ainoa järkevä vaihtoehto kulutustuote-käytössä. Passiivinen RFID-tunniste on tekniseltä tietoturvaltaan heikoin verrattuna muihin tunnisteisiin. (Sweeney II 2005, 39.)



Kuva 3. Passiivitunniste (Honkanen ym. 2009, 15).

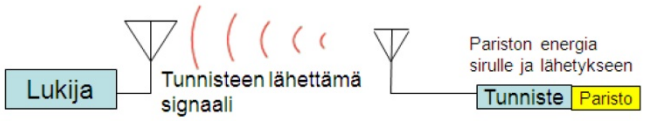
Mifare

Mifare on lyhyellä etäisyydellä toimiva RFID-sirutyyppi, joka on käytössä älykorteissa. Mifare-siru on Philipsin omistama ja se noudattaa ISO 1443 -standardia. Mifare-siru toimii 13,56 MHz:n LF-taajuudella. Sirun tiedonsiirto-nopeus on 106 kbit/s ja sen käyttöetäisyys lukijasta on korkeintaan 10 cm. Mifare-standardia käyttävä älykortti sisältää yhden tai neljän kilotavun EEPROM-muistin. Kortin pääasialliset käyttökohteet ovat julkisen liikenteen maksukortit tai kulunvalvontajärjestelmät. (Philips 2002, 3.) Philipsin tytäryhtiö NXP Semiconductors julkisti vuonna 2002 Mifare DESFire -tyyppisen

tunnisteen, jossa on keskitytty erityisesti tunnisteen turvaominaisuuksien kehittämiseen. (Philips 2008).

Aktiivitunnisteet

Aktiivitunniste vaatii oman virtalähteen toimiakseen (Finkenzeller 2003, 13). Tämä mahdollistaa kohteiden tunnistamisen pitkiltä etäisyyksiltä. Aktiiviset tunnisteet ovat passiivitunnisteita huomattavasti kalliimpia, joten niiden käyttö on tarkemmin harkittua ja perusteltua. Aktiivisten tunnisteiden hyviä puolia ovat pitemmät luku- ja kirjoitusetäisyydet, jotka ovat tyypillisesti noin 10 metriä. Aktiiviset tunnistimet ja lukijat toimivat aina joko VHF- tai UHF-taajuusalueilla. (ToP Tunniste, 2006.) Kuva 4 osoittaa, miten tunniste lähettää signaalia jatkuvasti, joten sen elinikä on kertakäyttöisen pariston vuoksi rajallinen. Käytettävistä tunnisteista aktiivitunniste on tiedonsiirtonopeudeltaan sekä tietoturvatasoltaan ylivoimainen verrattuna muihin tunnisteisiin. Aktiivitunnisteen komponenttien ja erikoisominaisuuksien takia se on markkinoilla olevista tunnisteista kallein. (Honkanen ym. 2009, 17.)



Kuva 4. Aktiivitunniste (Honkanen, Jalo & Kalliokoski 2009, 16).

Semi-passiiviset tunnisteet.

Semi-passiiviset tunnisteet eli BAP- (Battery Assisted Passive) tunnisteet ovat niin sanottuja hybriditunnisteita, koska niissä on sekä passiivi- että aktiivitunnisteiden positiiviset ominaisuudet. Tunnisteita käytetään pääosin erilaisiin anturisovelluksiin, kuten kylmäketjun seurantaan tai liiketunnistukseen. Tunnisteet soveltuvat erityisesti myös sovelluksiin, joissa vaaditaan tunnisteilta lisätehoa signaalin lähetykseen lukijalle. Esimerkiksi täyden trukkilavan keskimmäiset tuotteet eivät kykene passiivitunnisteilla lähettämään tietoa lukijoille, joten käytetään BAP-tunnistetta. Semi-passiivinen tunniste sisältää

oman virtalähteen kuvan 5 tapaan, mutta sitä ei käytetä kommunikointiin antennin kanssa, joten tunnisteiden käyttöikä on aktiivitunnisteita pidempi. Virtalähdettä käytetään edellä mainitun lisätehon saavuttamiseksi. (Sweeney II 2005, 38.)

Kuva 5. Semi-passiivitunniste (Honkanen ym. 2009, 17).

Tunnisteiden muistit

RFID-tunnisteet voidaan jakaa myös niiden muistityyppien mukaan eri kategorioihin. On olemassa kaksi päämuistityyppiä: read-only (RO) ja read/write (RW). Lisäksi muistityypeillä on variaatioita, kuten WORM sekä EEPROM. (Hunt ym. 2007, 8).

Oikean muistityypin omaava tunniste valitaan käyttötarkoituksen mukaan. Passiivisen muistin koko on 64 tavusta yhteen kilotavuun ja aktiivimuistin koko on korkeintaan 128 kilotavua. (ZEBRA Technologies 2010.)

Read only on muistityyppi, joka sisältää ainoastaan valmistusvaiheessa kirjoitetun EPC-koodin, jota ei voi muuttaa jälkikäteen. Muistin toiminta perustuu siihen, että siihen liitetyt toiminnot haetaan taustajärjestelmästä. (Association for Automatic Identification and Mobility 2010.) Kauppojen varashälyttimet sisältävät tämän tyyppisen RFID -tunnisteen. Kauppaesimerkissä tunnisteita on mahdollista kierrättää aktivoimalla ne uudestaan.

Read/Write-muistityypin omaaviin tunnisteisiin on mahdollista kirjoittaa ja lukea tietoa. Tästä syystä tunnisteita on mahdollista kierrättää erilaisissa kohteissa niiden uudelleenohjelmointimahdollisuuden ansiosta. (Association for Automatic Identification and Mobility 2010.)

WORM (Write Once Read Many) -muistityyppinen tunniste on vain kerran ohjelmoitavissa, mutta sitä on mahdollista lukea useita kertoja. Tämäntyylisiä

muistityyppejä kannattaa suosia järjestelmissä, joissa tarvitaan monia eri ominaisuuksilla varustettuja tunnisteita. (Association for Automatic Identification and Mobility 2010.)

EEPROM (Electrically Erasable Programmable Read-Only Memory) -muistityyppiset tunnisteet ovat monikäyttöisempiä verrattuna Read-Only -muistilla valmistettuihin tunnisteisiin. Tunnisteiden valmistusvaiheessa niihin ei tallenneta mitään tietoja, vaan käyttäjä ohjelmoi tunnisteen muistin haluamallaan tavalla ennen käyttöönottoa EPC -koodista lähtien. EEPROM -tyyppiset tunnisteet ovat Read-Only -muistityyppisiä tunnisteita kalliimpia johtuen niiden monimutkaisemmasta tekniikasta. Jos passiivisissa tunnisteissa halutaan käyttää tallennusmahdollisuutta, on valittava muistityyppi yleensä EEPROM. EEPROM on puolijohdemuisti, joka ei tarvitse virtaa säilyttääkseen siihen tallennetut tiedot. (Association for Automatic Identification and Mobility 2010.)

2.1.2 Lukijat

RFID-lukija on laite, joka lähettää radioaaltoa tunnisteille sekä vastaanottaa signaalin tunnisteelta. Lukija muuntaa analogisen signaalin digitaalisiksi binääriluvuiksi. Jokainen lukija on yhdistetty yhteen tai useampaan lukuantenniin. Lukija muodostaa ympärilleen sähkömagneettisen kentän, josta antenni lähettää signaalin eteenpäin. Varsinainen lukija välivarastoi antennilta kerätyt tiedot tarvittaessa ja syöttää ne taustajärjestelmään mahdollisuuden tullessa. (Bhatt & Glover 2006, 108.)

Markkinoilla on niin kiinteitä kuin mobileja lukijoita. Kiinteät lukijat voivat olla porttimaisia kuten kauppakeskuksen varashälyttimet. Suurikokoiset lukijat ovat tehokkaita, joten niillä on suuri toimintasäde. Tällaisia suuria lukijoita voidaan käyttää esimerkiksi satamissa tavarakonttien tunnistamiseen. Kannettavia käsilukijoita käytetään tilanteissa, joissa halutaan lukijan kanssa mennä tuotteiden luokse. Käsilukija on hyvä apuväline esimerkiksi kauppojen inventointeihin. Käsilukijat voivat kommunikoida taustajärjestelmän kanssa montaa eri yhteysvaihtoehtoa käyttäen: lukija on mahdollista kytkeä

tietokoneessa sijaitsevaan telakkaan USB- tai sarjaporttikaapelilla tai voidaan muodostaa yhteys suoraan taustajärjestelmään käyttäen WLAN- tai Ethernet-verkkoa. Lukijan käyttötarkoituksesta riippuen virta voi olla joko kytkettynä (varashälyttimet) tai tarvittaessa kytkettävissä (käsilukijat). (Bhatt & Glover 2006, 108.)

2.1.3 Taustajärjestelmä

Toimivaan järjestelmäkokonaisuuteen kuuluu aina palvelin, jota pidetään informaation säilytyspaikkana. Palvelimeen on syötetty järjestelmän kannalta tärkeitä tietoja, kuten lukijoiden tiedot sekä tunnistettavien kohteiden tiedot. (Bhatt & Glover 2006, 141.) Palvelimella toimiva ohjelmisto voi olla esimerkiksi SAP -toiminnanohjausjärjestelmä. Taulukko 1 kuvaa kulunvalvontajärjestelmiin tallennettuja tietoja, joista voidaan tarvittaessa tulostaa raportteja.

Taulukko 1. Kulunvalvontaesimerkki.

ID (EPC-koodi)	LUKUTAPAHTUMA-AIKA	TOIMINTA	PAIKKA
02.0000A23.00027B.0002983745DR7	19.08.2010, klo 7:30	Login_Aalto	ICT-talo, ovi 3
02.0000A23.00027B.0005433745DR7	19.08.2010, klo 8:28	Login_Lumme	ICT-talo, ovi 16
02.0000A23.00027B.000298374AQ3	19.08.2010, klo 18:23	Logout_Raitio	Lemminkäisenkatu, ovi 7
02.0000A23.00027B.000298374FDB3	19.08.2010, klo 19:59	Logout_Seppälä	ICT-talo, pääovi

2.2 Taajuudet

Radioaallot ovat taajuusalueen 3 Hz – 300 GHz välillä tapahtuvaa sähkömagneettista säteilyä. Taajuudella tarkoitetaan radioaallon värähtelyn määrää aikayksikössä. 1 Hz vastaa yhtä aaltoa sekunnissa ja 1 kHz vastaa tuhatta aallon värähtelyä sekunnissa. Mitä suurempi aallonpituus on, sitä alhaisempi on sen taajuus. Tunnisteet käyttävät LF-, HF-, UHF- ja mikroaaltotaajuuksia. Järjestelmät voidaan jakaa myös taajuusalueiden määrittämien lukuetäisyyksien mukaisesti kolmeen eri lajiin: close-coupling (0,1cm), remote-coupling (0-1m) ja long-range (>1m) -järjestelmiin.

(Finkenzeller 2003, 13.) Jokaisella taajuusalueella on etunsa ja haittansa. Taajuusalue on siis valittava käyttötarkoituksen mukaan.

Yleisillä radioaalloilla tapahtuvaan tiedonsiirtoon on jaettu taajuusalueet tiettyihin käyttötarkoituksiin. Esimerkiksi on päätetty, että GSM-verkko käyttää Euroopassa 900 MHz- ja 1800 MHz-taajuuksia. Yleisin käytössä oleva RFID:n käyttämä taajuus on tällä hetkellä 125 kHz. Häiriöiden minimoimiseksi on määritetty erityiset ISM-taajuudet (Industrial-Scientific-Medical), joita alun perin suunniteltiin käytettäviksi teollisuus-, tieteis- sekä terveydenhuolto-sovelluksissa. RFID- järjestelmät on suunniteltu toimimaan edellä mainituilla ISM-taajuuksilla, joiden käyttö ei vaadi erillisiä lupia. (Honkanen ym. 2009,13.) Yhdysvalloissa on käytössä 900 MHz:n taajuudet järjestelmissä, joten sieltä haluttaisiin tuoda tämä taajuus myös Eurooppaan. Ongelmana ovat kuitenkin päällekkäiset taajuudet GSM-verkkojen kanssa. Yhteiseksi ratkaisuksi on kuitenkin löytymässä 868 MHz:n alueella toimiva taajuus. Taajuuksilla on merkitystä lukuetäisyyksiin ja tiedonsiirtokapasiteettiin. Korkeammat taajuudet mahdollistavat pidemmät etäisyydet ja tehokkaammat tiedonsiirto-ominaisuudet. (Ekström 2001.)

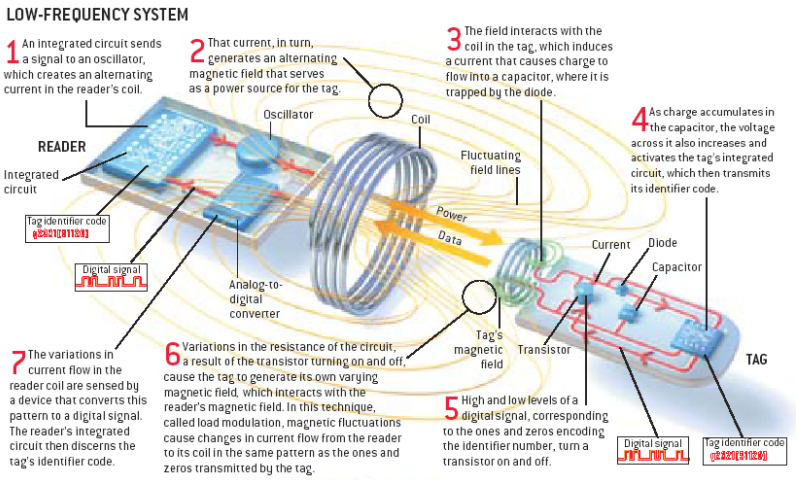
Kuten yleensä radiosignaalien kanssa, ympäristötekijät vaikuttavat suuresti järjestelmien lukuetäisyyksiin. Erityisesti niihin vaikuttavat lukijan ja tunnisteiden välissä olevat materiaalit. HF- ja UHF-taajuuksilla tapahtuva kommunikointi häiriintyy helposti vedestä ja metallista. Esimerkiksi kosteat materiaalit heikentävät merkittävästi signaalia tai voivat katkaista koko yhteyden. (Garfinkel & Rosenberg 2005, 26.) Yhteenveto RFID:ssä käytettävistä radiotaajuuksista on taulukossa 2 sivulla 21.

2.2.1 LF

LF (Low Frequency) on välillä 30 kHz – 300 kHz toimiva radioaaltotaajuus. Tämän alueen aallonpituus on 1 – 10 km. LF -taajuudella toimivat tunnisteet käyttävät yleensä 125 kHz:n tai 134 kHz:n taajuuksia. Nykyään käyttö rajoittuu lähinnä kulunvalvontaan ja eläinten tunnistamiseen. LF-taajuuden heikkouksia

on sen hidas tiedonsiirtokyky ja lyhyet lukuetäisyydet. Tästä syystä sen suorituskyky ei ole riittävä uusiin kehitteillä oleviin sovelluksiin.

LF- ja HF-taajuudet muodostavat lukijan kanssa induktiivisen kytkennän samalla tavoin kuin muuntajat. Tunnisteessa ja lukijassa on kuparinen käämi ja ne toimivat antenneina. Voidaan siis todeta, että passiiviset LF-radiotaajuutta käyttävä tunniste ei itsenäisesti kaiuta radioaaltoja. (Scher 2004.)



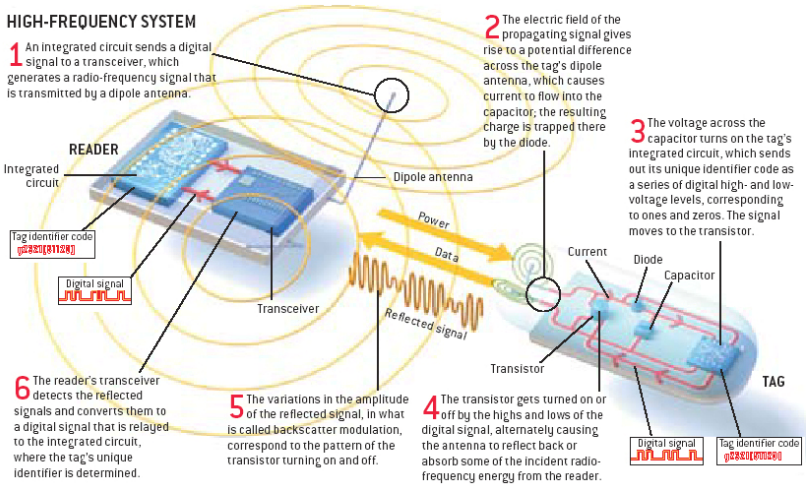
Kuva 6. LF-tunnisteen toiminta (Want 2004, 59).

Kuvassa 6 on havainnollistettu, kuinka LF-järjestelmän lukija ja tunniste kommunikoivat keskenään. Lukijaan integroitu piiri lähettää signaalin lukijan oskillaattorille eli värähtelijälle. Oskillaattori synnyttää vaihtovirran lukijan käämille. Vaihtovirran avulla saadaan aikaiseksi magneettikentän muutokset, mikä taas toimii tunnisteen virtalähteenä. Magneettikenttä toimii tunnisteen käämin kanssa, mikä vastaavasti indusoi vastaanotetun vaihtovirran, ja kondensaattori saa virran jännitteen muutoksesta ja päästää virran lävitseen diodille. Kondensaattorin vastaanottaessa virtaa sen läpi kulkeva jännite kasvaa samalla, mikä aktivoi tunnisteen integroidun piirin ja lähettää tunnistekoodin lukijalle. Koodi lähtee digitaalisena signaalina tunnisteen transistorille, joka kytkimen tapaan joko päästää signaalin läpi tai pysäyttää sen. Digitaalielektroniikasta tutut 0 ja 1 toimivat transistorin käskyinä (1 = on ja 0 = off). Mikäli lukija ja tunniste ovat tarpeeksi lähellä toisiaan ja tällöin jännite on transistorille riittävä (1), päästää transistori signaalin yhä edelleen kohti lukijaa.

Mikäli taas tunniste on liian kaukana lukijasta, jää jännite alhaiseksi ja tällöin transistori saa alhaisen signaalin (0) eli portti (looginen) jää kiinni. Tunnisteen magneettikenttä toimii yhdessä lukijan magneettikentän kanssa. Lukijan kentän avulla tunniste saa virran ja tunnisteen kentän avulla lukija saa datan. Data siirtyy tunnisteesta lukijaan analogisesti magneettikentän mukana ja lukijan muunnin muuttaa signaalin takaisin digitaaliseen muotoon. Lukijan integroitu piiri tunnistaa digitaalisen tunnisteen lähettämän koodin. (Want 2004, 59.)

2.2.2 HF

HF (High Frequency) käsittää 3 – 30 MHz:n taajuuksilla toimivia radioaaltoja, joiden aallonpituus välillä 10 m – 100 m. RFID:n yhteydessä HF-taajuudella tarkoitetaan 13,56 MHz alueella toimivaa radioaaltoa, joka on kansainvälisesti vapaa taajuus. HF-taajuus on kehittyneempi LF-taajuuteen verrattuna sen laajemman lukuetäisyyden ja nopeamman tiedonsiirtokapasiteettinsa takia. Vastaavasti se myös tarvitsee enemmän energiaa toimiakseen kuin LF-taajudella toimiva tunniste. HF-tunnisteet sisältävät niin sanotun muuntajan LF-tunnisteiden tapaan, eivätkä ne lähetä radioaaltoja. (Scher 2004.) HF-taajuutta on käytetty esimerkiksi kirjastojen aineiston hallinnassa ja tavaroiden inventointia helpottavien järjestelmien tunnisteissa.



Kuva 7. HF-tunnisteen toiminta (Want 2004, 59).

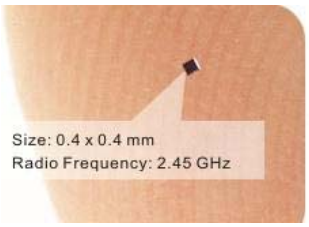
Kuvassa 7 on nähtävissä, kuinka HF-taajuudella toimiva tunniste ja lukija kommunikoivat keskenään. Lukija lähettää digitaalisignaalia tunnisteelle dipoliantennin välityksellä. Etenevä signaali kasvattaa magneettikentän voimakkuutta kulkiessaan tunnisteen dipoliantennin lävitse, mikä aiheuttaa sähkön siirtymiseen kondensaattoriin, josta diodi saa tarvittavan latauksensa. Kondensaattorin lävitse kulkeva jännite muuttuu, minkä jälkeen se ottaa käyttöön tunnisteessa olevan integroidun piirin. Tämä lähettää lukijalle uniikkia tunnuskoodiansa digitaalisen jännitteen vaihteluna, josta muunnetaan binääriluku. Tämän jälkeen binääriluku siirtyy transistoriin. Transistori kytkeytyy päälle tai pois binääriluvun ykkösten ja nollien tavoin. Lukijaan on määritelty binäärilukujen merkitykset, eli kumpi arvo imee signaaleja ja kumpi hylkii niitä. Lukijan lähetinvastaanotin tunnistaa heijastuneet signaalit ja muuntaa ne digitaaliseksi signaaliksi, minkä jälkeen ne muutetaan vielä binääriluvuiksi, ja tämän jälkeen lukija pystyy tunnistamaan lähettimen. (Want 2004, 59.)

2.2.3 UHF

UHF (Ultra High Frequency) -taajuus toimii 300 MHz:n ja 3 GHz:n välillä ja 10 cm – 1 m aallonpituudella. RFID-tunnisteet toimivat 866 – 960 MHz:n taajuudella. Euroopassa käytettävät taajuudet ovat 869 MHz:n tietämillä ja Yhdysvalloissa käytetään 902 – 928 MHz:n taajuuksia. UHF-tekniikkaa voidaan verrata radioon, koska siinä välitetään radioaaltoja. Tiedonsiirto-ominaisuuksiltaan UHF-taajuusalueella toimivat toteutukset ovat kokonaisuudessaan edellä mainittuja LF- ja HF-tekniikoita kehittyneempiä. UHF -tunnistamisessa on mahdollista käyttää nopeampaa datasiirtoa pidemmillä etäisyyksillä. UHF-tekniikka jakautuu kahteen tyyppiin: far field ja near field -tekniikkaan (FF ja NF). Haastavissa olosuhteissa, kuten kosteissa oloissa tai metallisten rakenteiden ympärillä pystytään käyttämään NF-tunnisteita niiden signaalien hyvän läpäisykyvyn ansiosta. Vastaavasti FF-tekniikkaa ei pystytä käyttämään kosteissa ja metallisissa olosuhteissa. Tulevaisuudessa NF UHF -tekniikkaa käytetään tuotteiden tunnistamiseen LF-tekniikan sijaan. (Scher 2004.)

2.2.4 Mikroaallot

Mikroaallot ovat korkeataajuisia elektromagneettisia aaltoja, joiden pituus vaihtelee 0,1 – 30 cm. Aallonpituudet ovat radioaaltoja lyhyemmät, mutta pidemmät kuin infrapuna-aallot. Mikroaallot jaetaan käyttötarkoituksen mukaan eri taajuusalueisiin. Mikroaalloiksi lasketaan UHF, SHF (Super High Frequency 3 – 30 GHz), EHF (Extremely High Frequency 30 – 300 GHz) ja alimillimetrisäteily (submillimetrialue 300 – 3000 GHz). Mikroaaltojen ja radioaaltojen raja on liukuva ja siksi myös UHF-taajuuksia käsitellään niin radio- kuin myös mikroaaltoina. Siksi mikroaallot liittyvät osittain myös UHF-taajuuksilla toimivaan RFID-tekniikkaan. Mikroaaltotaajuuksia käytetään enimmäkseen aktiivitunnistuksessa, kuten tietulleissa. Mikroaaltotunnisteet toimivat yleensä 2.4 GHz:n tai 5,8 GHz:n taajuuksilla. (Scher 2004.) Kuvassa 8 on rakenteeltaan maailman pienin RFID- tunniste. Tämä tunniste toimii mikroaalloilla.



Kuva 8. Mikrotagi Hitachi μ-Chip (Hitachi 2010).

Yleisesti mikroaaltoja käytetään tutkissa ja mikroaaltouuneissa. Mikroaalloilla on todella hyvä tiedonsiirtokyky, mutta samalla ne kuluttavat hyvin paljon virtaa ja ovat ratkaisuina kalliita. Yleensä puhuttaessa mikroaalloilla toimivasta tiedonsiirrosta tarkoitetaan WLAN-tekniikkaa. WLAN voi usein toimia yhdessä RFID-tekniikan kanssa. Mikroaalloilla toimivia tunnisteita voidaan lukea jopa kymmenen metrin etäisyydeltä.

Taulukko 2. Taajuusalueiden vertailua (Kranenburg & Ward 2006, 10).

KANAVA	LF	HF	UHF	MIKROAALLOT
TAAJUUS ALUEET	30 - 300kHz	3 - 30MHz	300MHz - 3GHz	2 - 30GHz
RFID - TAAJUUDET	125 - 134kHz	13,56MHz	* 433MHz, 865 - 956MHz, 2,45GHz	2,45GHz
STANDARDIT	ISO 18000-2	ISO 18000-3	- ISO 18000-4 - ISO 18000-6 - ISO 18000-7	- ISO 18000-4
LUKUETÄI-SYYDET	~ 0.5 m	~ 1,5m	- 433HMz max 100m 865 - 956MHz~ 0,5 - 5m	~ 10m
TIEDONSIIRTO NOPEUDET	< 1kt/s	~ 25kt/s	433 - 956MHz = 30kt/s 2,45GHz = 100kts/s	> 100kt/s
OMINAISUUDET	- lyhyt lukuetäisyys, - hidas tiedonsiirto, - läpäisee veden muttei metallia	- pidempi lukuetäisyys (vrt. LF) - nopeampi tiedonsiirto (vrt. LF) - läpäisee veden muttei metallia	- pitkä lukuetäisyys - nopea tiedonsiirto - 100 kohteen samanaikainen luku mahdollinen - ei läpäise vettä, eikä metallia	- pitkä lukuetäisyys - nopein tiedonsiirto - ei läpäise vettä, eikä metalleja
ESIMERKKI-SOVELLUKSIA	- eläinten sirutus - varkaudenesto järjestelmät	- kirjastojärjestelmät - matkakortit - kulkukortit	- logistiikkaketjut - jakeluketjujen hallinta	-tietullit

Taulukosta 2 voi havaita eri taajuusalueiden keskeisiä ominaisaisuuksia sekä vertailla niitä keskenään.

3 NFC – NEAR FIELD COMMUNICATION

NFC (Near Field Communication) -tekniikka on lyhyen kantaman langattomien yhteyksien standardi, joka on suunniteltu intuitiiviseen, vaivattomaan ja samalla turvalliseen kommunikointiin elektronisten laitteiden välillä. (NFC forum 2010c). Tekniikka perustuu RFID-tekniikan kanssa samaan ISO 14443 -standardisarjaan. NFC-tekniikka toimii 13,56 MHz taajuudella. Tekniikassa on käytössä kolme eri tiedonsiirtonopeutta: 106, 212 tai 424 kilobittiä sekunnissa. (Mazo 2009, 1.)

NFC-laitteiden välinen yhteys syntyy, kun kaksi laitetta on toistensa lähietäisyydellä, jolloin magneettikentän induktio aktivoituu niiden välille. Sama NFC-laite voi toimia sekä lukijana että tunnisteena. Lukuetäisyydet NFC-tekniikassa ovat hyvin lyhyitä, mutta toisaalta juuri sen takia saavutetaan korkea tietoturvataso. Lukuetäisyydet pysyvät alle kahdessakymmenessä senttimetrissä ja ovat yleensä noin 10 senttimetriä. Onnistunut varmennus edellyttää näköyhteyttä lukijan kanssa. NFC-tekniikan sovellukset yleistyvät jatkuvasti ja lisää sovelluksia kehitetään elämän eri osa-alueille soveltuviin

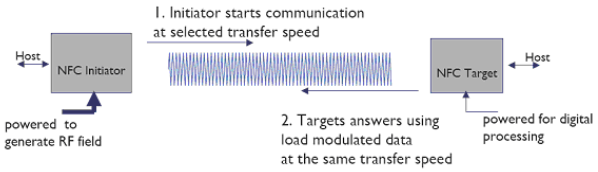
käyttötarkoituksiin jatkuvasti. Suurimmaksi osaksi sovelluksia hallitaan matkapuhelimien avulla. NFC-matkapuhelin sisältää niin RFID-tekniikasta tutuksi tulleen lukijan kuin tunnisteen. NFC-laitteet voivat kommunikoida RFID-laitteiden tapaan kahdella eri tavalla, joko passiivisesti tai aktiivisesti. (Mazo 2009, 2; Ciruela ym. 2010, 72.)

Voidaan sanoa, että NFC on eräänlainen trendi maailmalla, mutta kehittyneissä Aasian maissa tekniikasta on tullut jo jokapäiväinen maksuväline. NFC-sovellusmaailmaan kuuluu muun muassa myöhemmin esitettävien kontaktittomien maksutapojen lisäksi helppo ja nopea tiedonsiirto, joka mahdollistaa pääsyn esimerkiksi digitaalisiin aineistoihin tunnisteita koskettamalla. (NFC Forum 2010c.) Vuonna 2009 Nokia julkaisi markkinoille NFC-ominaisuudella varustetun matkapuhelimen malliltaan Nokia-6212.

Kuva 9. Nokia 6131 NFC-puhelin (Nokia 2010).

3.1 Passiivitila

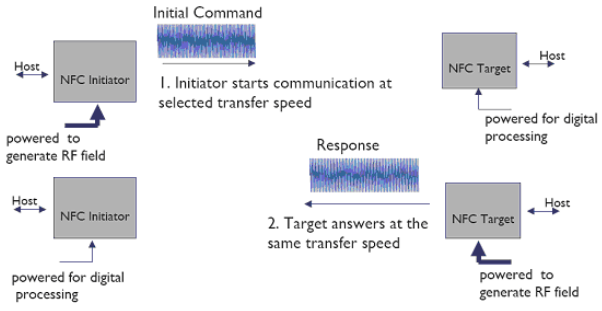
Kuvasta 10 voidaan havaita, kuinka passiivinen tunniste ei muodosta omaa sähkömagneettista kenttäänsä eikä sillä ole myöskään omaa virtalähdettä. Passiivisessa tilassa oleva laite saa virtansa toisen laitteen muodostamasta sähkömagneettisesta kentästä. NFC-älykortti on hyvä esimerkki laitteesta, jossa on passiivinen NFC-siru. (Mazo 2009, 2.)



Kuva 10. Passiivisen NFC-yhteyden toimintaperiaate (Mazo 2009, 2).

3.2 Aktiivitila

Aktiivisessa tilassa oleva NFC-laite (kuva 11) muodostaa aina oman sähkömagneettisen kenttänsä. Aktiivisilla NFC-laitteilla on yleensä oma virtalähde. Aktiivisessa tilassa lähettäjä pakkaa energian ja lähetettävän tiedon samaan signaaliin, jonka jälkeen signaali lähetetään vastaanottajalle. Vastaanottaja käsittelee lähettäjän pyynnön ja pakkaa energian ja tiedon myös samaan signaaliin ja palauttaa sen lähettäjälle. (Mazo 2009, 3.)



Kuva 11. Aktiivisen NFC-yhteyden toimintaperiaate (Mazo 2009, 3).

3.3 Lyhyen kantaman langattomat tiedonsiirtomenetelmät

NFC-tekniikka luo kuluttajalle vaivattomamman ja nopeamman tavan kommunikoida eri laitteiden välillä. Infrapunatekniikka, joka kehitettiin vuonna 1993, oli maailman ensimmäinen langaton yhteystyyppi. Infrapunayhteydellä oli mahdollista kommunikoida esimerkiksi kahden matkapuhelimen tai tietokoneen ja matkapuhelimen välillä. Yhteys on hyvin herkkä ulkoisille häiriötekijöille, koska se vaatii suoran näköyhteyden laitteiden välille. Esimerkiksi kirkas valo saattaa heikentää infrapuna-aaltoa ja aiheuttaa näin ongelmia infrapunayhteyteen. Vaikka Bluetooth-tekniikassa on nopeampi tiedonsiirtokapasiteetti verrattuna infrapunatekniikkaan, niin Bluetooth-yhteyden haittapuolena on yhteydenmuodostamisen hitaus. Yhteyden luominen laitteiden välille tapahtuu parittamalla (coupling). (Paus 2007, 11.) Langattomien tiedonsiirtomenetelmien eroja ja yhtäläisyyksiä vertaillaan taulukossa 3.

Taulukko 3. NFC-, Bluetooth- ja infrapunayhteyksien vertailua (Paus 2007, 12).

	NFC	NFC -EDUT	BLUETOOTH	INFRAPUNA
YHTEYS-TYYPPI	Point-toPoint	- helppo muodostaa - toimii lyhyillä etäisyyksillä	Point-to-Multipoiint	Point-to-Point
TOIMINTA-AUE	< 0,1m	- turvallinen, esim täydessä metrossa. - signaalia on vaikea kaapata	< 10m	~1m
TIEDONSIIRTO-NOPEUS	424 kt/s * 848 kt/s (tulossa 1megatavun yhteys)		721 kt/s	115 kt/s
YHTEYDEN MUODOSTAMINEN	< 0,1s	- helppo ja nopea maksaminen esim julkisessa liikenteessä.	6s	0,5s
TUNNISTETYYPPI	- aktiivi-passiivi - aktiivi-aktiivi	Lukija toimii myös lähettimenä (matkapuhelin)	aktiivi-aktiivi	aktiivi-aktiivi
RFID YHTEENSOPIVUUS	kyllä	toimii erilaisissa ympäristöissä, hyödyntää olemassa olevaa RFID -tekniikkaa	ei	ei
KUSTANNUKSET	edullinen		kalliimpi	halpa

3.4 CASE: Tukholma

Vuonna 2008 TeliaSonera ja ASSA ABLOY -konsernin tytäryhtiö VingCard demostroivat Tukholmassa hankkeen, jonka tavoitteena oli tuoda magneettiraidalla toimivan hotelliavaimen rinnalle mahdollisuus käyttää NFC-puhelinta avaimena. Käytännössä sisäänkirjautumisen yhteydessä asiakkaan NFC-puhelin aktivoitaisiin toimivaksi hotellin tietojärjestelmän kanssa. (Hospitality.net 2008.) Käytännössä idea toteutui vasta marraskuun alussa 2010, jolloin konsepti näki päivänvalon tukholmalaisessa Clarion-hotellissa neljän kuukauden mittaisen pilotin muodossa. Hotellivieraat saavat käyttöönsä NFC -ominaisuuden sisältävän matkapuhelimen, jonka avulla he voivat kirjautua hotelliin sisälle, eikä vastaanotossa tarvitse erikseen asioida. Lisäksi puhelin toimii hotellihuoneen avaimena. (Vaalisto 2010.) Todennäköisesti vastaavanlainen toiminto on mahdollisesti tulossa myöhemmin yritysten kulunvalvontajärjestelmiin.

3.5 CASE: Lontoo

Lontoossa sijaitsevassa Newham Collegessa käynnistettiin kesäkuussa 2010 hanke, jossa 120 opiskelijaa ja neljä opettajaa saivat käyttöönsä NFC-etätunnistustekniikalla varustetut matkapuhelimet kuukauden ajaksi. Tuntien alkaessa opettajat kirjautuvat luokkahuoneeseen omalla puhelimellaan, jolloin he aktivoivat kyseisen huoneen tilankäyttö- ja oppilaiden läsnäolorekisterin. Oppilaat saavat läsnäolomerkinnän tietokantaan, kun opettaja heilauttaa puhelintaan oppilaiden NFC-kulkukorttien läheisyydessä. Järjestelmän on kehittänyt suomalainen Reslink Solutions Oy. (Balaban 2010a.)

3.6 CASE: Suomi

Luottokunta, Nokia, Visa Europe, sähköiseen varmennukseen erikoistunut Venyon ja Sodexo toteuttivat Suomessa vuonna 2009 Contactless Mobile Payment -pilotin, joka kesti kesäkuusta joulukuuhun. Näistä yrityksistä muodostettu kolmenkymmenen henkilön ryhmä käytti Nokia 6212 -puhelinta

maksamiseen Luottokunnan ja Nokian toimitaloissa olevissa kolmessa Sodexon lounasravintoloissa. Käyttäjillä oli mahdollisuus suorittaa alle 20 euron ostoksia ilman PIN-koodia. Visa payWave -maksusovellus (Visa Credit) ja Luottokunnan käyttöliittymä ladattiin Venyonin tuottamasta personoinnin mahdollistamasta OTA-palvelusta. (Alarto 21.9.2010, sähköpostiviesti.)

Pilottihanke oli onnistunut. Käyttäjille oli jäänyt positiivinen tunne palvelusta. Heidän mielestään tekniikka tuntui valmiilta ja palvelun tuleminen laajamittaisempaan käyttöön olisi tervetullutta. Maksaminen oli nopeaa ja luotettavaa. Lukija ilmoitti selkeästi vihreällä valolla ja opastetekstillä onnistuneesta maksusuorituksesta. Pilotin ongelmat rajoittuivat lähinnä käyttäjistä riippumattomiin yhteysongelmiin. Jotkut käyttävät tarvitsivat opastusta perusasetusten eli mobiilin Internet-liittymän asentamiseen. (Alarto 26.10.2010, sähköpostiviesti.)

3.7 NFC Forum

NFC Forum on voittoa tavoittelematon yhdistys, jonka tarkoituksena on kehittää sekä edistää NFC-tekniikan käyttöä. Foorumin forumin perustivat Philips, Nokia ja Sony vuonna 2004. Tällä hetkellä foorumissa on jo 140 jäsentä monilta erilaisilta tekniikkaa hyödyntäviltä aloilta. NFC Forumin tärkeimpiin tehtäviin kuuluu yhtenäisten standardien luominen NFC-laitteille. NFC-tekniikan standardoinnilla on samat päämäärät kuin RFID-tekniikan standardoinnilla eli NFC-laitteiden merkkiriippumattomuuden saavuttaminen. NFC-Forumin tehtävänä on myös järjestää tekniikkaan liittyviä koulutustilaisuuksia. (NFC forum 2010a.)

Jokaisella perustajajäsenellä on omat näkemyksensä NFC-tekniikan tulevaisuudesta; Philipsin mukaan NFC on tekniikka, joka mahdollistaa kuluttajille helpomman tavan päästä käsiksi eri alojen palveluihin. Nokian mukaan NFC on hieno tapa tuoda esille heidän käsitystään tulevaisuuden mobiilista maailmasta, jota Nokia itse edustaa. Sony näkee NFC-tekniikan rajapintana kaikkien elektronisten laitteiden ja ihmisten välillä. Sony markkinoi

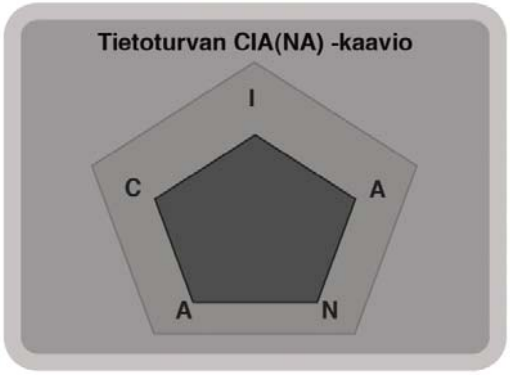
NFC:n yleistymisen puolesta kaikkiin elektronisiin laitteisiin eikä pelkästään matkapuhelimiin. (NFC Forum 2010b; Paus 2007.)

4 TIETOTURVA

Euroopan unionin talous- ja sosiaalikomitea antoi 27.10.2007 lausunnon RFID-tekniikasta todeten seuraavaa:

> ”Radiotaajuustunnistus ei ole vielä valmis tekniikanala, joten sen koko potentiaalia ei vielä ymmärretä. Toisaalta se voi hyödyttää suunnattomasti teknispohjaista kulttuuriamme, mutta toisaalta siihen liittyvä tekniikka saattaa aiheuttaa yksityisyyden suojalle ja vapaudelle ennennäkemättömän suuren uhan.” (Dimitriadis 2007, 67.)

Tietoturva on osa-alue, joka kuuluu alaan kuin alaan ja eritoten tietoteknillisissä sovelluksissa merkitys on kriittinen. Tietoturva on laajamittainen kokonaisuus ja se käsittelee lukuisia eri osa-alueita. RFID/NFC -järjestelmissä on neljä suojattavaa tahoa: tunnisteissa ja lukijan muistissa oleva data, tunnisteiden ja lukijoiden välinen tiedonsiirto ja tietoa käsittelevät järjestelmät esim. palvelimet. (Bhutani, M & Moradpour S. 2005, 106–107.) Yleisesti tietoturvakokonaisuus voidaan pilkkoa monella eri tavalla pienempiin osiin ja yleisin jako on kuvion 1 esittämä CIA-kolmio ja sen laajennettu muoto CIA(NA). Lisäksi tietoturva voidaan jakaa kahdeksaan eri osa-alueeseen. OSI-malli on myös tapa, jolla jakaa kokonaisuus tasoittain omiin lokeroihin. Tietoturvaa ei voida liiaksi korostaa: se on osana kaikkea, haluamme sitä tai ei, ja jos sitä ei oteta tosissaan, saattaa aiheutua suurimittaisia vahinkoja.



Kuvio 1. CIA(NA)-kaavio.

Kuvion 1 C-kirjain kuvastaa tietojen luottamuksellisuutta (confidentiality). Tiedot, järjestelmät ja palvelut ovat vain niihin oikeutettujen saatavissa eikä niitä saa luvatta paljastaa tai muutoin saattaa sivullisten tietoon. I-kirjain esittää kuviossa tietojen eheyttä (integrity). Tiedot, järjestelmät tai palvelut eivät ole laitteisto- tai ohjelmistovikojen, luonnontapahtumien tai oikeudettoman inhimillisen toiminnan seurauksena muuttuneet tai tuhoutuneet. Kuvion ensimmäinen A-kirjain kuvastaa tietojen saatavuutta (availability). Tiedot, järjestelmät ja palvelut ovat aina niihin oikeutettujen tahojen hyödynnettävissä. N-kirjain esittää tietojen kiistämättömyyttä (nonrepudiation). Sähköisessä viestinnässä kiistämättömyydellä tarkoitetaan toimenpiteitä, joilla varmistutaan viestin lähettäjästä ja vastaanottajasta. Kuvion toinen A-kirjain voi kuvastaa pääsynvalvontaa (access control), joka on muista poiketen tapa hallita aiemmin mainittuja tukipilareita (CIA-triangle). (Viestintävirasto 2009.)

Tietoturvan osa-alueet

Suomessa valtiovarainministeriön VAHTI (Valtionhallinnon tietoturvallisuuden johtoryhmä) on määritellyt ohjeistuksia tietoturvallisuudesta ja se määrittelee tietoturvallisuuden seuraavasti:

> ”Tietoturvallisuus on sekä toimintojen ja palveluiden edellytys että säädösvelvoite. Valtionhallinnon tietoturvallisuus on laaja kokonaisuus, jonka toimenpidealueet on jaoteltu seuraaviin osa-alueisiin: hallinnollinen tietoturvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus, tietoliikenneturvallisuus, ohjelmistoturvallisuus, tietoaineistoturvallisuus ja käyttöturvallisuus." (Helsingin seudun kauppakamari 2010.)

Kuvio 2. Tietoturvan osa-alueet.

Kuviosta 2 voidaan tarkastella tietoturvan laajuutta ja todeta sen yltävän fyysisestä turvallisuudesta aina tietoliikenneturvallisuuteen saakka. Jokainen osa-alue on tärkeä eikä ainuttakaan tule unohtaa, mutta puhuttaessa etätunnistustekniikoista nousee väkisinkin tietoliikenneturvallisuus ylitse muiden.

Tietoliikenneturvallisuuden tavoitteina on varmistaa viestien alkuperäisyys, koskemattomuus ja luottamuksellisuus. Lisäksi tulee todentaa niin lähettäjä (tunniste) kuin vastaanottaja (lukija). Osa-alueen päämääriin kuuluu myös viestinnän yksityisyys ja yksityisyyden suoja. Toki tietoliikenneturvallisuuden alle kuuluu myös tietoliikennelaitteiden fyysinen turvallisuus.

Tietoliikenneuhkia on monenlaisia ja usein ne ovat kriittisiä ja toteutuessaan saattavat aiheuttaa laajamittaista haittaa. Tunnisteisiin kohdistuvat

käytettävyyttä vastaan tehdyt hyökkäykset, kuten palvelunestohyökkäykset, ovat uhka, joka tulee huomioida jo suunnitteluvaiheessa ja pohtia oikeaa ratkaisua. Lisäksi luottamuksellisuutta uhkaavia hyökkäyksiä, kuten datan sieppausta ja salakuuntelua, vastaan tulee suojautua muun muassa kryptografian avuin. Eheyttä vastaan kohdistuvat hyökkäykset eli kulkevan signaalin luvaton muuttaminen ja häirintä saattavat tulla vastaan RFID/NFC-sovelluksia käyttäessä. Jopa henkilötiedot saattavat olla vaarassa ja joutua väärien tahojen haltuun, mikäli ei olla tarkkoja esimerkiksi uusien biometristen passien suunnitteluvaiheessa. Voidaan siis todeta, että tietoliikenneturvallisuus koostuu CIA(NA) -kaavion periaatteista, niihin mahdollisesti kohdistuvista hyökkäyksistä ja niiden ehkäisemisestä.

OSI-mallin tasot

Taulukko 4. OSI-kerrokset ja RFID (Banks ym. 2007, 118).

DATA UNIT	LAYERS	DESCRIPTION (WHERE APPLICABLE IN RFID)
DATA	APPLICATION	- Sends or retrieves applications to or from tags
DATA	PRESENTATION	- Data representation - Data encryption
DATA	SESSION	- Manages and terminates connection between transmitting and receiving ends. - Not applicable in RFID
SEGMENTS	TRANSPORT	- Controls the reliability of data transfer between users. - Not applicable in RFID, since there are no complex links involved.
PACKETS	NETWORK	- Network routing and flow control. - Not applicable in RFID, since all links are point-to-point.
FRAMES	DATA LINK	- Transmission of data blocks. - Address management, error detection and correction.
BITS	PHYSICAL	- Manages physical interface between tag and reader. - Defines data rate, encoding, and modulation schemes.

Taulukosta 4 voidaan havaita, kuinka tietoliikenneturvallisuus on mahdollista pilkkoa tasoihin OSI-mallin (Open Systems Interconnection Reference Model) mukaisesti. OSI-malli on ympäristö- ja verkkoprotokollan suunnittelun looginen kuvaus, joka koostuu 7 kerroksesta (layers). Jokaisella kerroksella on omat tehtävät ja velvollisuudet. Tietoturva kulkee mukana jokaisella kerroksella ja siksi OSI -protokolla onkin oiva tapa pohtia RFID/NFC -tekniikan tietoturvaa ja sen sisältämiä ongelmia. Yllä olevasta taulukosta selviää, miten RFID/NFC-

ympäristö sijoittuu kerroksille (RFID:ssä käytössä tasot 1,2,6 ja 7). Fyysinen kerros (physical layer) sisältää radioaallot, jotka toimivat rajapintana tunnisteen ja lukijan välillä. Rajapinta tulee suojata mahdollisilta hyökkäyksiltä. Siirtokerros (data link layer) mahdollistaa tietoliikennepakettien lähetyksen. RIFD-järjestelmissä verkkokerroksella (network layer) ei ole käyttöä, koska kommunikointi on point-to-point-tyylistä, eikä täten signaalia tarvitse reitittää välikäsien kautta. Kuljetuskerrostakaan (transport layer) ei tarvitse ottaa huomioon puhuttaessa RFID-maailmasta. Istuntokerros (session layer) huolehtii prosesseista, kuten operaatioiden uudelleenkäynnistämisestä ja keskeytyksestä, mutta nämä asiat eivät liity RFID-viestintään. Myöskään kerrokselle kuuluva kanavointi (multiplexing) ei liity yhteyden muodostukseen. Esitystapakerros (presentation layer) huolehtii tunnisteen lähettämän signaalin koodaamisesta sellaiseen muotoon, että käytössä oleva tietokoneohjelmisto osaa tulkita sen. Sovelluskerroksen (application layer) tehtävänä on toimia rajapintana käyttäjien tunnisteen ja lukijan välillä. (Banks ym. 2007, 117–118.)

Yleisimmät tietoturvariskit RFID-tekniikassa

Yleisempiä tietoturvariskejä ja aukkoja RFID/NFC-liikenteessä on tunnisteiden luvaton jäljittäminen, lukeminen ja kloonaaminen. Lisäksi lukijan ja tunnisteen välinen tiedonsiirron salakuuntelu (eavesdropping) on mahdollista, mikäli asiaa ei huomioida alusta alkaen. (Glover & Bhett 2006, 197–214.) Tunnisteista saatetaan pystyä lukemaan tietoja käyttäjän tietämättä ja useimmiten puhutaan salakuuntelusta. Mikäli yhteydessä ei käytetä asiaan kuuluvaa salausta, on signaalin kaappaus mahdollista. Kommunikoinnin pystyy salaamaan melko yksinkertaisesti esimerkiksi salasanoin ja PIN-koodein. Mikäli halutaan salausominaisuuksia itse tunnisteeseen, niin tunnisteelta vaaditaan niin sanottua lisä-älyä, joka taas nostaa tunnisteen valmistuskustannuksia. Toisaalta salakuuntelua rajoittavat myös lyhyet lukuetäisyydet ja heikot signaalit. Heikkojen signaalien salakuuntelu on mahdollista, mutta se vaatii erillisiä salakuuntelulaitteita tunnisteen läheisyyteen, jolloin salakuuntelu onkin erittäin hankala toteuttaa. Fyysisesti signaaleja voidaan myös suojata sijoittamalla

järjestelmä niin sanotun Faradayn häkin sisälle, mistä ulkopuoliset eivät kykene kaappaamaan signaalia. (Järvinen 2007.)

Epäeettinen seuranta on ehkä subjektiivinen käsitys, mutta yleensä otsakkeen alle lasketaan muun muassa liiallinen kellokorttimainen käyttäytyminen työpaikkaympäristöissä, asiakkaiden kulutuskäyttäytymisen seuranta markkinointitarkoituksissa ja ihmisten seuraaminen esimerkiksi nykyisten biometristen tunnisteiden avulla. Sen lisäksi, että tunnisteen ja lukijan välistä liikennettä saatetaan seurata käyttäjän tietämättä, on olemassa riski tunnisteen väärentämiseen. Puhuttaessa väärentämisestä on kyseessä tunnisteiden kloonaus (cloning), jossa aidosta tunnisteesta tehdään jäljennös ja sitä käytetään erilaisissa eettisesti epäilyttävissä tai jopa laittomissa aikeissa. Kloonauksen uhkaa ei pidä vähätellä ja siksi onkin olemassa erilaisia ratkaisuja uhan minimoimiseksi. Uhkaa voidaan kiertää käyttäen niin sanottuja muuttuvia autentikointimenetelmiä. Muuttuva autentikointimenetelmä voi olla esimerkiksi sellainen, jossa tunnisteen autentikointivastaus riippuu lukijan antamasta avaimesta. Tunniste siis sisältää algoritmin, joka laskee autentikointivastauksen lukijan antaman avaimen perusteella. Tällöin pelkkä tunnisteen kommunikointiviestien kloonaus ei riitä, koska autentikointivaiheessa tunnisteen vastaus on aina erilainen, riippuen täysin lukijan antamasta avaimesta. Pelkkä tunnisteen kloonaaminen ei siis auttaisi vierailijaa, koska vaadittaisiin myös autentikointialgoritmin murtamista. (Glover & Bhett 2006, 211.)

Edellä mainittujen uhkien lisäksi mahdollisia ovat myös Internetistä tutuksi tulleet palvelunestohyökkäykset (Denial of Service, DoS), joiden tarkoituksena ei ole tunkeutua järjestelmän sisälle ja kaapata liikkuvaa dataa, vaan ainoastaan häiritä tai jopa estää liikenteen kulkua. Järjestelmien viestintää on mahdollista häiritä käyttäen avuksi sähkömagnetiikkaa. Muita häiriötä aiheuttavia asioita ovat muun muassa nesteet, metallit, ilmankosteus ja langattomat verkot. (Bhutani & Moradpour 2005, 49.)

5 STANDARDIT

RFID:n nopea kehitys edellyttää jatkuvia muutoksia ja mukautuksia tekniikoihin, tuotteisiin ja palveluihin. Standardien ja niiden laatimisprosessin on pysyttävä nopealiikkeisten maailmanmarkkinoiden tahdissa. Näin ollen palvelujen sujuvan käyttöönoton kannalta on olennaisen tärkeää, että kansainvälisiä standardeja saadaan hyväksyttyä nopeutetulla tahdilla ja alueellisia standardeja saadaan yhdenmukaistettua. Keskeisellä sijalla on myös RFID-toimintoja tukevien tietojärjestelmien yhteensopivuus, varsinkin kun tavoitteena on luoda sähköisille palveluille avoimet Euroopan laajuiset markkinat. (EUR Lex 2007.)

Eri yrityksien kehittämät, samaan käyttötarkoitukseen rakennettujen laitteiden hinnat ovat laskeneet kilpailutilanteen synnyttyä. (RFID Lab Finland 2010.) Yhteisistä sopimuksista riippumatta kaikki alalla toimivat yritykset eivät ole noudattaneet standardeja, minkä seurauksena käyttäjille on aiheutunut ongelmia tuotteiden käytössä. Standardien luomisen ongelmana on ollut myös lainsäädäntöjen ristiriitaisuus, koska jokainen maa on voinut määritellä RFID-tekniikassa käytettävät radiotaajuudet jo valmiiksi muihin käyttötarkoituksiin. RFID-standardeja kehittävät ISO (International Organization for Standardization), EPCglobal, ETSI (European Telecommunications Standards Institute) ja yhdysvaltalainen FCC (Federal Communications Commission). Standardijärjestöjen olemassaolosta huolimatta Euroopassa ja Yhdysvalloissa olevat standardit ovat ristiriidassa. (Honkanen ym. 2009, 23.)

Standardit on jaoteltu neljään pääryhmään:

- tiedonsiirto
- tiedon esitystapa ja koodaus
- testaus
- yhteensopivuus. (Kranenburg & Ward 2006, 11.)

RFID-laitteiden tiedonsiirrossa käytettävät taajuudet on määritelty ISO 18000 -ilmarajapinta standardisarjassa. Tunnisteen sirun tietosisältö on määritetty standardissa ISO-11784. Sirun tiedonsiirtotaajuus määritellään standardeissa

ISO 11785 ja ISO 18000. Aikaisemmin standardien määrä oli paljon suurempi, koska esimerkiksi tietulleille, eläintentunnistuksille ja älykorteille oli nimetty omat standardit. Tällä hetkellä tekniikoiden sovellustavalle haetaan standardeja sovellutuksen käyttämän taajuusalueen mukaan. (Kranenburg & Ward 2006, 12.) RFID-tiedonsiirrossa käytettävät ISO:n ilmarajapintastandardit on taulukossa 2 sivulla 21.

Vuonna 1999 kansainvälistä toimintaa koordinoimaan perustettiin Auto-ID Center ja sen päätarkoituksena oli kehittää EPC-standardia sekä sen tekniikkaa. Kehitystyön tuloksia olivat yhtenäinen tiedonsiirtomenetelmä, tunnisteen tietosisällön liittäminen EPC-standardin omaavaan tunnisteeseen sekä toimivan verkkoinfrastruktuurin luominen palvelemaan tiedon säilyttämistä ja siirtoa kansainvälisesti eri toimijoiden välillä.

Standardointityö on vuodesta 2003 lähtien ollut EPCGlobalin tehtävänä, koska Auto-ID Center suljettiin. Standardointityön yhtenä päämääränä on RFID-tekniikan kehittäminen sellaiseksi, että se palvelee yrityksiä mahdollisimman hyvin kansainvälisessä liiketoiminnassa. Tekniikkaa kehitettäessä on aina pidetty tärkeänä yritysten ja yksityisten henkilöiden yksilönsuojan ja tietoturvan säilyminen.

Suurin osa LF-alueen sovelluksista, kuten esimerkiksi kulunvalvontajärjestelmät on toteutettu suljettuina järjestelminä 125 kHz taajuuksilla. Karjan tunnistukseen on vastaavasti määritelty standardi ISO11784, joka määrittää tunnisteen tietosisällön ja ISO11785, joka määrittelee tiedonsiirtoprotokollan 134 kHz taajuudella. (RFID Lab Finland 2010.)

HF taajuusalueelle 13,56 MHz:n taajuudelle on myös luotu standardeja. ISO14443-standardin luomisen tarkoituksena oli mahdollistaa eri valmistajien tunnisteiden ja lukijoiden yhteensopivuus, mutta standardin tämän hetkinen käyttö ei ole valitettavasti saavuttanut sen kaikkia mahdollisia etuja. (RFID Lab Finland 2010.) Tarkempia tietoja RFID-tekniikkaan liittyvistä standardeista saa ISO:n tai EPCGlobalin kotisivuilta www.iso.org & www.epcglobalinc.org.

6 JURIDIIKKA

Niin kansalliset kuin kansainvälisetkin lait pyritään aina muotoilemaan tekniikasta riippumattomiksi sekä myös uusiin innovaatioihin helposti sovellettavaksi. Näin ollen RFID/NFC -etätunnistustekniikasta puhuttaessa on tiedostettava, että niitä koskevat lukuisat eri lait, joista esimerkkeinä henkilötietolaki, kuluttajansuojalaki sekä sähköisen viestinnän tietosuojalaki. EU asettaa perussopimuksillaan ja asetuksillaan minimivaatimukset jäsenmaidensa kansallisille lainsäädännöille. Direktiiveillään EU tarkentaa lakeja mutta samalla antaa jäsenmaille luvan tarkentaa sääntöjä parhaalla katsomallaan tavalla. EU on huomioinut direktiivejään säätäessään myös uusien innovaatioiden kehittymisen. Uusia lakeja ei tarvitse siis säätää aina uuden tekniikan tullessa markkinoille. Lisää lakikokonaisuuksista voi lukea Suomen osalta Finlexistä http://www.finlex.fi tai Euroopan osalta EURLexistä http://eur-lex.europa.eu/.

Henkilötietolaki

> Tämän lain tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista (Henkilötietolaki 22.4.1999/523 § 1).

> Henkilötiedoilla tarkoitetaan kaikenlaisia luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, joista voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan samassa taloudessa elävät ihmiset. Henkilötietoja keräävän tahon on perusteltava asianomaiselle, että miksi hän tarvitsee nimenomaisesti näitä tietoja rekisteriin. (Henkilötietolaki 22.4.1999/523 § 3.)

> Rekisterinpitäjän tulee käsitellä henkilötietoja laillisesti, noudattaa huolellisuutta ja hyvää tietojenkäsittelytapaa sekä toimia muutoinkin niin, ettei rekisteröidyn yksityiselämän suojaa ja muita yksityisyyden suojan turvaavia perusoikeuksia rajoiteta ilman laissa säädettyä perustetta. Sama velvollisuus on sillä, joka itsenäisenä elinkeinon- tai toiminnanharjoittajana toimii rekisterinpitäjän lukuun. (Henkilötietolaki 22.4.1999/523 § 5.)

Kuluttajansuojalaki

> Tämä laki koskee kulutushyödykkeiden tarjontaa, myyntiä ja muuta markkinointia elinkeinonharjoittajilta kuluttajille. Lakia sovelletaan myös, kun elinkeinonharjoittaja välittää hyödykkeitä kuluttajille. Tämä laki ei koske lakisääteisiä vakuutuksia eikä työntekijän ryhmähenkivakuutusta tai sitä vastaavaa kunnallisen eläkelaitoksen myöntämää etuutta. (Kuluttajansuojalaki 20.1.1978/38 § 1.)

Sähköisen viestinnän tietosuojalaki

> Lain tarkoituksena on turvata sähköisen viestinnän luottamuksellisuuden ja yksityisyyden suojan toteutuminen sekä edistää sähköisen viestinnän tietoturvaa ja monipuolisten sähköisen viestinnän palvelujen tasapainoista kehittymistä (Sähköisen viestinnän tietosuojalaki 16.6.2004/516 § 1).

Laki yksityisyyden suojasta työelämässä

> Tämän lain tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia työelämässä (13.8.2004/759 § 1).

> Työntekijöihin kohdistuvan kameravalvonnan, kulunvalvonnan ja muun teknisin menetelmin toteutetun valvonnan tarkoitus, käyttöönotto ja valvonnassa käytettävät menetelmät sekä sähköpostin ja muun tietoverkon käyttö sekä työntekijän sähköpostin ja muuta sähköistä viestintää koskevien tietojen käsittely kuuluvat yhteistoiminnasta yrityksissä annetussa laissa, yhteistoiminnasta valtion virastoissa ja laitoksissa annetussa laissa sekä työnantajan ja henkilöstön välisestä yhteistoiminnasta kunnissa annetussa laissa tarkoitetun yhteistoimintamenettelyn piiriin. Muissa kuin yhteistoimintalainsäädännön piiriin kuuluvissa yrityksissä ja julkisoikeudellisissa yhteisöissä työnantajan on ennen päätöksentekoa varattava työntekijöille tai heidän edustajilleen tilaisuus tulla kuulluiksi edellä mainituista asioista. (Laki yksityisyyden suojasta työelämässä 13.8.2004/759 § 21.)

Yllä olevat lait määrittelevät hyvin tarkkaan säännöt työnantajan mahdollisuuksista valvoa työntekijöitänsä elektronisesti. Teknisesti työnantajan olisi mahdollista seurata reaaliaikaisesti työntekijän liikkumista. Euroopan komission suosituksen mukaan työnantajan täytyy informoida työntekijöilleen tarkasti tiedoista, mitä tietoja ja mihin tarkoituksen työnantaja käyttää kulunvalvontajärjestelmästä saamaansa informaatiota. Työnantaja ei saa pitää tiedoista salaisia tietokantoja, vaan hänen on vaadittaessa näytettävä työntekijälle häntä koskevat tiedot. (RFID Europe 2009.) RFID-tekniikan avulla työpaikalla mahdollisesti tapahtuvaa epäeettistä seurantaa voidaan verrata muutaman vuoden takaiseen keskusteluun LEX-Nokiasta, jolloin sähköpostiliikenteen tunnistetietojen seuraamisesta nousi suurta kohua.

Kauppojen ja kauppakeskuksien täytyy kertoa asiakkailleen etätunnistusjärjestelmien käytöstä sekä selvittää niiden tarkoitus. Tähän riittää yleensä liikkeen ulkopuolella oleva ilmoitus, jossa kerrotaan siellä käytettävästä elektronisesta tuotesuojauksesta varkauden varalta.

Jotta käyttäjät hyväksyisivät uudet tekniikat, tarvitaan selkeät ja ennakoitavat oikeudelliset ja poliittiset puitteet. (Dimitriadis 2007.) Tulevaisuudessa saattaa siis olla tarvetta tarkentaa jo olemassa olevia lakeja ja asetuksia.

7 PÄIVÄN TILANNE KOTITALOUKSISSA

Sekä RFID- että NFC -tekniikka ovat hiljattain saavuttaneet suuren yleisön eli kotitaloudet. Tähän päivään asti RFID/NFC on ollut tapa toteuttaa asioita yrityksissä ja suurissa toimitusketjuissa (supply chain). Tekniikan käyttö ja hyödyntäminen jokapäiväisessä elämässä on vasta murrosvaiheessa. Kulunvalvonta eli erilaiset kulkukortit sekä erilaiset hälyttimet ja anturisovellukset ovat suurimpia kokonaisuuksia, joissa RFID-tunnistamista on käytetty yksityisten kuluttajien piirissä. Esimerkiksi Turun ammattikorkeakoulussa on käytössä RFID-tekniikkaan perustuva kulunvalvontajärjestelmä.

Maailmanlaajuisesti kotitalouksille suunnatut järjestelmät ja sovellukset ovat rantautuneet ensin Amerikan Yhdysvaltoihin muun muassa tietullien muodossa. Nykyään myös Ranskan Liber-T - tietullijärjestelmä perustuu RFID-tunnistukseen. Lisäksi samalla tekniikalla on toteutettu erilaisia vaihtoehtoja perinteisille maksutavoille, joista myöhemmin lisää. Edellä mainittuja maksutapoja aletaan hiljalleen myös siirtää toimivaksi matkapuhelinympäristössä ja tällöin puhutaan NFC-maksusuorituksista.

Yhdysvaltojen lisäksi sovellusmaailman huippua on jo pitkään ollut Aasian maaperällä ja eritoten Japanissa ja Kiinassa. Aasiassa kontaktittomat maksutavat ovat jo osana arkea, ja muun muassa Hong Kongissa toimiva Octopus Card on maailmankuulu älykortti (smart card). Euroopassa sovellukset ovat hieman kehityksessä jäljessä verrattuna Yhdysvaltoihin ja Aasiaan. Hong Kongin Octopus -korttiin voidaan verrata toista maailmakuulua julkisen palvelun Oyster Cardia Lontoossa. Lisäksi vastaavia kortteja on niin Saksassa (VRR/VRS Card) kuin Hollannissakin (OV-chipkaart).

Toisaalta taas tekniikan tutkimus ja kehitystyö on maailman kärkeä ja muun muassa Suomessa on panostettu hurjasti itse tekniikan tutkimukseen ja kehittämiseen. Myös konkreettisten laitteiden ja tunnisteiden valmistuksessa kunnostautunut Suomi nousee esille puhuttaessa RFID/NFC-tekniikasta. Jottemme unohtaisi Australiaa & Oceaniaa sekä Afrikkaa, puhumattakaan Etelä-Amerikasta, todettakoon, että Australiassa on jonkin verran sovelluksia käytössä ja käynnissä on lukuisia pilottihankkeita. Afrikka tulee huomattavasti muita maanosia perässä, mutta muun muassa satamien avuksi on kehitelty nykyaikaisia RFID-järjestelmiä. Kotitalouksille suunnatut sovellukset Afrikan maaperällä jäävät silti käytännössä biometristen passien varaan. Etelä-Amerikassa sijaitsevassa Brasiliassa sijaitsevissa yliopistoissa tehdään laajamittaista tutkimus- ja tuotekehitystyötä.

Tekniikka ei ole lyönyt itseään läpi suuressa mittakaavassa ja löytyy lukuisia eri syitä, joista varmasti käyttäjätahojen tiedon puute on yksi suurimmista. Uuden tekniikan tuomat järjestelmät ovat usein kalliita, ja siksi rahoittajatahot haluavatkin kuulla tarkkoja arvioita tekniikan takaisinmaksuajoista. Useasti ollaan skeptisiä uusista tekniikoista ja niiden luotettavuudesta. RFID-ympäristöä pystyttämässä olevat tahot pelkäävät, ettei uudistuksesta saadakaan irti haluttuja tehoja ja hankkija jäisi tappiolle. Euroopan komission komissaari Viviane Redingin mukaan tekniikasta saataisiin irti kaikki sen tarjoama hyöty, jos eri maiden yritykset tekisivät tiiviimmin yhteistyötä ja jakaisivat tietotaitoa sekä kokemuksia. (Schindler 2009, 4.) Kuluttajalle voi herätä kysymyksiä liittyen hänen yksityisyydensuojaansa. Kuluttaja pelkää, että häntä tarkkaillaan ja hän saattaakin ajatella, että onko hän enää turvassa missään ja keneltäkään. Ubiikkimaailma (ubiquitous computing) eli esineiden Internet on tuloillaan, ja radiotaajuustunnistus on suuressa roolissa näissä innovaatioissa.

On tutkittu, että mitä positiivisempi asenne ihmisellä on tietotekniikkaa kohtaan, sitä positiivisempi asenne tulee olemaan RFID-tekniikkaa kohtaan. Lisäksi ihmisten mielipiteiden RFID-tekniikasta uskotaan korreloivan heidän mielipiteisiinsä tunnisteita sisältävistä tuotteista. Toisin sanoen, mitä positiivisempi asenne ihmisellä on RFID-tekniikkaa kohtaan, sitä positiivisempi

on hänen asenteensa tuotteita kohtaan, jotka sisältävät tunnisteen. Yleinen uskomus on, että ihmisten asenteet kulkevat käsi kädessä käyttäytymisen kanssa. Mitä positiivisempi asenne ihmisellä on RFID-tekniikkaa kohtaan, sitä positiivisemmin hän käyttäytyy tekniikkaa ja sitä hyödyntäviä tuotteita kohtaan. Mitä positiivisemmin ihminen asennoituu RFID-tunnisteen sisältäviin tuotteisiin, sitä positiivisemmin hän suhtautuu niiden ostamiseen ja käyttämiseen. Luultavasti ihmisillä ei ole vielä vahvoja mielipiteitä RFID:stä. Ihmiset tulevat asennoitumaan tekniikkaan sen mukaan, minkälainen tuote tulee sisältämään tunnisteen. (Boslau & Lietke 2005.) Tuskin ihmiset välittävät maitopurkissa olevasta RFID-tunnisteesta, mutta varmasti on tuotteita, joiden hankkimista ei haluta seurattavan.

7.1 Tilanne Suomessa

Nokia on nostanut Suomesta varteenotettavan teknologiavaltion suurten jättien, kuten Yhdysvaltojen ja Japanin, rinnalle. Suomessa on jo pitkään ollut alan osaamista ja tietotaitoa.

> ”Tuskin nokialaiset olisivat menestyneet niin hyvin, jos he olisivat jääneet 1980-luvulla odottamaan, millaisia matkapuhelimia Ericsson ja Motorola saavat aikaiseksi” (Nurminen, T, 2005).

Nokian kaltainen veturi uupuu yhä RFID-markkinoiltamme ja tienraivaus on yhä käynnissä. Toisten mielestä Suomi on aivan kärkimaita RFID-maailmassa, mutta asiasta on esitetty myös eriäviä mielipiteitä. Suomi on antanut korkean panoksen RFID-tekniikan kehitykseen ja koulutukseen. Suomessa toimii muutamia konsultointi-instansseja, joiden tarkoituksena on löytää tienraivaajia tekniikan käyttöönottoon. Voidaan kuitenkin todeta, että Suomi on vielä lastenkengissä, kun puhutaan RFID/NFC-maailman sovelluksista. Suomessa ei ole tekijöitä, jotka olisivat halukkaita olemaan se ensimmäinen suuri kokeilija. Suurimmaksi osaksi se johtuu siitä, että ollaan skeptisiä RFID:n tuomista hyödyistä, eikä olla tietoisia tekniikan takaisinmaksuarvioista. On selvää, ettei kukaan ole valmis ottamaan käyttöön uutta tekniikkaa, jonka tuotoista ja hyödyistä ei ole selkeää kuvaa. Onneksi kuitenkin itse tietotaito tekniikkaa kohtaan on huipputasoa ja Suomessa on joukko kouluttautuneita alan

ammattilaisia. Kun tietotaito saadaan siirrettyä myös mahdollisille käyttäjille eli yrityksille, ovat ovet auki.

Suomessa on myös käynnissä lukuisia pilottihankkeita, joissa on kokeiltu tekniikan käyttöä mitä erilaisimmissa ympäristöissä. Pilottihankkeet ovat jokseenkin kansalaisilta pimennossa, eikä niitä kaikkia haluta esitellä julkisesti. Julkinen liikenne on suurin tiedossa olevista alueista, jossa RFID-tekniikka on käytössä tai sen käyttöönottoa on vakavasti harkittu.

Kaupunkikorttihankkeet

Suomessa julkisen liikenteen maksujärjestelmää on kehitetty siten, että perinteisten maksutapojen rinnalle on otettu käyttöön RFID-etämaksukortteja. Korteille on ollut mahdollista ladata joko kerta- tai kausikortteja. Tällaisia paikallisliikenteen järjestelmiä on käytössä useissa kaupungeissa Suomessa. Oulun kaupunki oli maailman ensimmäinen kaupunki, joka otti käyttöön RFID-tekniikkaan perustuvan bussikortin vuonna 1986. Helsingin seutuliikenteen matkakorttia pystytään käyttämään busseissa, raitiovaunuissa, metroissa ja VR:n lähiliikenteessä. Jotkut kaupungit ovat kehittäneet bussikorteista monikäyttöisiä kaupunkikortteja.

Meneillään on muutamia hankkeita liittyen kaupunkikorttijärjestelmiin ja niiden päivitykseen. Suomessa FinnCity2-kaupunkikorttihankkeessa on mukana Mikkeli, Pori, Oulu ja Vantaa (Oulun kaupunki 2010). Vantaa kuuluu myös Helsingin seutuliikenteen matkakortin piiriin (HSL Helsingin seudun liikenne 2010). Myös Turun kaupungilla on käytössä linja-autoissa ja kaupungin liikuntapaikoissa etäluettavia Arvokortteja (Turku 2010). Näitä kortteja ei ole ainakaan vielä yhdistetty, vaikka se olisi teknisesti mahdollista. Vuoteen 2009 asti jopa kaupungin uimahalleihin ja Kupittaan urheiluhalliin oli erilliset kortit.

FinnCity2-projektin käynnistämiseen päädyttiin, koska monella kaupungilla todettiin olevan samantapaisia tavoitteita kaupunkikorttiensa kehittämiseen. Oulun kaupungin tarjoamalle OuluCardille on mahdollista ladata bussilippuja, liikuntapaikkojen sarjakortteja sekä kirjaston palveluja. Vuonna 2011 kortin palveluvalikoimaa laajennetaan ja turisteille tullaan tarjoamaan muun muassa

turistilippua. Turistilipulle on mahdollista ladata muun muassa bussi- sekä kulttuuripalveluiden pääsylippuja. Oulun kaupungin työntekijöillä OuluCard toimii lisäksi avainkorttina ja työpaikkaruokalan maksukorttina. Oulu ottaa OuluCardin toisen version käyttöön syksyllä 2010. Uusi kortti on halvempi ja kestävämpi verrattuna aiempaan korttiin. Uusi kortti on ISO/IEC 14443 -standardiin pohjautuva Mifare Desifire RFID-etäkortti. Kortti on myös huomattavasti kestävämpi rakenteeltaan kuin edeltäjänsä. Keskinarkauksen mukaan suurimmat säästöt kaupunkikorttihankkeissa saadaan käyttöönoton jälkeen manuaalisen työn vähenemisen ansiosta. Esimerkiksi teatterissa käytettävän paperilipun kappalehinnaksi on laskettu kaikkine kuluineen noin 2 – 4 €/kpl sisältäen lipun suunnittelun, painatuksen sekä manuaalisen laskennan ja tilityksen. Sähköistä kaupunkikorttia käyttämällä lippujen käsittelykuluiksi on arvioitu 0,40 - 1,00 € /lippu. (Keskinarkaus 13.9.2010, sähköpostiviesti.)

Oulussa on kaupunkikorttihankkeen kanssa samaan aikaan menossa myös eurooppalainen ITEA2 SmartUrbanSpaces -projekti. Projekti on yhteishanke, jossa on mukana yksitoista kaupunkia neljästä eri maasta. Kolmivuotisen projektin tavoitteena on kehittää yhteensopivia, helppokäyttöisiä kaupunkipalveluja hyödyntäen uusinta mobiiliteknologiaa sekä tietotekniikkaa. Pääpaino hankkeessa on luoda kaupunkien välisellä yhteistyöllä eurooppalaisia palvelukokonaisuuksia, toimintatapoja ja standardeja, joiden pohjalta kaupungin asukkaille pystytään kehittämään parempia mobiilipalveluita (Oulun kaupunki 2010).

Kuva 12. Lajitelma eri kaupunkien kaupunkikorteista.

Kuvassa 12 nähdään muun muassa uusi Tampereen julkisten palvelujen älykortti eTampere, joka on FinnCity-hankkeen kaltainen kaupunkikorttiprojekti. eTampere-korttihankkeessa käytetty pilottikortti on niin sanottu hybridikortti, jossa samaan muoviin on yhdistetty ISO 14443 -standardin mukainen RFID-siru sekä ISO 7816 -standardin mukainen kontaktillinen sirukortti. Kontaktillinen siru sisälsi kaksi avainparia (julkinen ja salainen avain) sekä niiden käyttöön vaadittavat PIN-tunnukset. eTampere-korttipilottia ei ole suunniteltu tarkasti rajattuihin palveluihin. Jokaisella kortin haltijalla on yksilöllinen eTampere elektroninen tunniste eli EETU. Tällä tunnisteella käyttäjä pystyy asioimaan niin verkossa kuin fyysisessä ympäristössäkin. Verkossa käyttäjä pystyy hallitsemaan kortilla olevia palveluita. eTampere-korttia on pystytty käyttämään joissain paikallisissa palveluissa myös luotettavana henkilöllisyystodistuksena. Valtakunnallisesti on puhuttu paljon elektronisesta äänestyksestä. Tampereen ammattikorkeakoulun edustajistovaaleissa on kokeiltu sähköistä äänestämistä, eTampere-kortin siruominaisuutta. Tämä hanke onnistui teknisesti hyvin. Tämän perusteella voisi olla mahdollista, että tulevaisuudessa valtakunnallisella, virallisella henkilökortilla olisi toteutettavissa sähköinen äänestys. (Tampereen kaupunki 2005.)

Biometrinen passi

Biometrinen passi (biometrical passport), on biometrisen tunnisteen sisältävä, aikaisempaa passia turvallisempi matkustusasiakirja. Sen käyttöönotto on EU-maiden yhteinen hanke, jonka tavoitteena on tehdä passien väärentämisestä ja väärinkäytöstä entistäkin vaikeampaa. (Poliisi 2010a.) Biometrinen passi sisältää RFID-tunnisteen, jolle on tallennettu tietoja passin omistajasta, kuten henkilön nimi, henkilötunnus, kansalaisuus, passinhaltijan kasvokuva, nimikirjoitus ja digitaalinen allekirjoitus. Suomessa tiedot suojataan valtion digitaalisella allekirjoituksella, joka varmistaa, että sirulla on vain myöntäjäviranomaisen tallentamia tietoja. (Poliisi 2010b.) Se, mitä mainituista tiedoista passi sisältää, riippuu passin myöntäjämaan asettamista määräyksistä. Suomalaisesta biopassista löytyy kuitenkin kaikki edellä mainitut tunnistetiedot. RFID-tunniste on sijoitettu passin henkilötietosivun sisälle ja se sisältää niin

sirun kuin antennin. Tunniste pohjautuu ISO/IEC 1443-standardiin ja sillä on vähintään 32 kB:n EEPROM-muisti (maakohtainen). Sirun toimintaa ja sinne tallennettavia tietoja suojataan lukuisilla turvaratkaisuilla. BAC (Basic Access Control) suojaa passin sirun ja lukijan välistä liikennettä. Kaikki valtiot eivät ole ottaneet tätä ominaisuutta käyttöön jostain syystä. Passive Authentication (PA) suojelee passin sirulla olevaa tietoa ja se on määritetty pakolliseksi kaikkiin biopasseihin. Active Authentication (AA) -ominaisuuden tarkoituksena on estää passin tietosirun kloonaaminen. EU:n alueella myönnettyihin passeihin on lisätty myös muita turvaominaisuuksia, jotka eivät kuulu biometrisen passin alkuperäiseen standardiin. (Sisäministeriö 2010.) Yhdysvallat ovat lisänneet passin kanteen ohuen metallilevyn (Shielding the chip), joka estää passin lukemisen sen kannen ollessa kiinni. Näin ollen passeja ei voida skannata esimerkiksi lentokentillä. (Kleiner 2005.) Kaikista passin turvaominaisuuksista huolimatta saksalaiset tietoturvatutkijat Adam Laurie ja Jeroen van Beek pystyivät murtamaan biometrisen passin turvaominaisuudet (Korkimo 2008).

Biometrisen passin standardi ICAO 9303 on sama kuin ISO/IEC 7501, mikä on kehitetty YK:n alaisen kansainvälisen siviili-ilmailujärjestön (ICAO) puitteissa. Standardin mukaan kaikkien biometristen passien tulee sisältää kasvokuva biometrisena tunnisteena. Lisäksi standardi sallii sormenjälkien ja iiriksen käytön biometrisina tunnisteina. Euroopan unionin biometrista passia koskeva asetus määrää jäsenmaat ottamaan käyttöön kasvokuvan ja sormenjäljet biometrisina tunnisteina. Biometrisen passin voimassa oloaika on viisi vuotta. (Sisäministeriö 2010).

Biometrisella passilla on tärkeä rooli identiteettivarkauksien, laittoman maahantulon, kansainvälisen terrorismin ja kansainvälisen rikollisuuden torjunnassa. (Gipp ym. 2007, 11.) Biometrian avulla rajavalvonta voidaan kohdistaa entistä paremmin: suurista matkustajavirroista voidaan tunnistaa ne ihmiset, jotka tulee ottaa tarkempaan tarkasteluun (Sisäministeriö 2010).

Maailmassa on 70 maata, joissa on käytössä biometrinen passi. Malesia myönsi maailman ensimmäiset biometriset passit vuonna 1998. Näissä passeissa oli ominaisuus, jonka avulla voitiin selvittää passinhaltijan

matkahistoriaa. EU:n alueella biometristen passien myöntäminen aloitettiin vuonna 2006. Pohjoismaissa Ruotsi ja Norja ehtivät ottaa biometriset passit käyttöön jo vuonna 2005 ennen Suomea, Islantia ja Tanskaa. Ne aloittivat passien myöntämisen toukokuussa 2006. (Sisäministeriö 2010.) Tutkimuksen aikana saatoimme tehdä mielenkiintoisia havaintoja biometristen passien liikkeellelaskujärjestyksestä. Suurimpina ihmetyksen aiheina olivat muun muassa se, että muutamissa Afrikan maissa on käytetty kyseisiä passeja yhtä kauan kuin osissa niin sanotuissa länsimaisissa sivistyksen maissa. Tuli myös eräänlaisena yllätyksenä, että suuret maat kuten Kanada ja Brasilia eivät ole ottaneet käyttöön vielä biometrisia passeja. Biopassien liikkeelle laskemisaikataulutuksesta on oma luettelonsa työn liiteosiossa (liite2).

Kuva 13. Biopassin rakenne (eGov 2010).

Kuvasta 13 voidaan havaita seuraavia biometrisen passin rakenteellisia ominaisuuksia:

1) muovipinta, joka suojaa henkilötietosivua
2) henkilötietosivu
3) RFID-tunniste
4) muovipinta
5) tunnisteen antenni
6) tunnisteella sijaitseva prosessori
7) tunnisteella oleva siru.

7.2 Tilanne ulkomailla

RFID/NFC-tekniikka on suuressa murrosvaiheessa maailmanlaajuisesti ja varsinkin NFC-tekniikan yleistyminen tuo tekniikan suuren yleisön eli kotitalouksien käyttöön. Vuonna 2005 Nurminen arvioi artikkelissaan, että niin USA:lla, Englannilla kuin Saksallakin olisi muutaman vuoden etumatka Suomeen verrattuna. Tutkimustulokset kuitenkin osoittavat, että Saksassa ei olisi ainakaan NFC-tekniikasta kovinkaan mittavia kokemuksia. (Nurminen 2005.) Maailmalla, eritoten Yhdysvalloissa ja Aasian teknologiamaissa, kontaktiton maksaminen (contactless payment) on lyönyt itsensä läpi, ja sitä varten onkin nykyään olemassa lukuisia eri wave & pay -ajatuksella toimivia maksukortteja. Aasiassa ja Amerikassa on osittain jo siirrytty tekniikan toiseen aaltoon eli päivittäiseen mobiiliin NFC-maksamiseen.

Kontaktittomien maksutapojen perustarkoituksena on tehdä ihmisten arjesta vaivattomampaa. Tekniikan avulla niin tiedon saanti, ostosten ja palveluiden maksaminen, julkisen liikenteen käyttö sekä tiedon jako helpottuu ja nopeutuu radikaalisti.

Exxon polttoainekortti

Maailman suurimpana öljyn tuottajana ja myyjänä tunnettu Yhdysvaltalainen ExxonMobil esitteli asiakkailleen kuvassa 14 esiintyvän RFID-avaimenperän (keychain RFID) vuonna 1997. Sen avulla voidaan asioida wave & pay -malliin yli 10 000 huoltoasemalla ympäri maailman. Kyseinen SpeedPass on ensimmäinen maailmanlaajuisesti käyttöönotettu RFID-maksujärjestelmä kuluttajille. SpeedPass-maksua testattiin monilla eri aloilla, kuten pikaruokaloissa ja supermarketeissa. Muun muassa McDonald's testasi SpeedPass-maksua yli 400 ravintolassaan Chicagon seudulla. Heidän pilottiinsa osoittautui kannattamattomaksi ja ominaisuus poistettiin käytöstä.

Kuva 14. SpeedPass -avaimenperä (ExxonMobil 2010).

Octopus Card – Hong Kong

Samana vuonna 1997 julkaistiin ja käyttöönotettiin kuvassa 15 esiintyvä Hong Kongin julkisen liikenteen Octopus Card. Maksukorttijärjestelmän suunnitteli australialaistaustainen ERG Group ja kortti perustuu Sonyn kehittämään 13,56 MHz:n taajuudella toimivaan FeliCa RFID-tunnisteeseen. Octopus Cardin tiedonsiirtonopeus on 212 kbit/s, joka on myös FeliCa-sirujen maksiminopeus. Lisäksi sillä on sisäänrakennettua muistia 1 Kb:sta aina 64 Kb:iin asti. Korttia pidetään yleisesti maailman ensimmäisenä kontaktittomana maksukorttina.

Kuluttajat voivat maksaa kortilla niin metro-, juna- kuin linja-automatkansa ja lisäksi se toimii maksuvälineenä lukuisissa eri liikkeissä, kuten lähikaupoissa, kioskeissa, supermarketeissa ja pikaravintoloissa. Kortilla voi maksaa myös Hong Kongin parkkiautomaateilla, huoltoasemilla ja erilaisilla

myyntiautomaateilla. Kaukoidän seudulla myös Shanghailla, Etelä-Korealla, Kiinalla ja Japanilla on käytössä samantyylisiä etäkorttiratkaisuja.

Octopus Card on saanut kansainvälistä tunnustusta muun muassa voittamalla World Information Technology and Services Alliancen myöntämän Global IT Excellence -palkinnon vuonna 2006. Kortti palkittiin maailman johtavana kompleksina automaattirahastus ja kontaktittomana älykortti -maksujärjestelmänä. Lisäksi Octopus Cards Limited sai tunnustusta korteissaan käytettävien tekniikkojen innovatiivisesta käytöstä. Vuoden 2009 arvion mukaan Octopus-kortteja on Hong Kongissa liikkeellä yli 17 miljoonaa, joka on yli kaksi kertaa Hong Kongin väkiluku. Yli 95 % Hong Kongissa asuvista käyttää Octopus-korttia ja suorituksia tapahtuu päivittäin yli 10 miljoonaa. Octopus on tuonut itseään kansainvälisesti tunnetuksi slogaanillaan Making Everyday Life Easier. (Octopus 2007.)

Kuva 15. Hong Kongin Octopus Card (Octopus 2007).

Oyster Card – Lontoo

Octopus Card ei suinkaan ole ainoa maailmanlaajuisesti tunnettu kontaktiton maksutapa ja maailmalla jopa tunnetumpi saattaa olla Lontoossa käytössä oleva kuvan 16 mukainen Oyster Card. Oyster on vuonna 2003 käyttöönotettu Lontoon julkisen liikenteen maksukortti. Octopus Cardin tapaisesti Oyster Card toimii maksuvälineenä niin Lontoon metroissa, linja-autoissa, Docklandin alueen automaattimetroissa (Docklands Light Railways, DLR), London Overground -rautatiejärjestelmässä, joissakin jokiristeilypalveluissa kuin myös useimmissa kansallisissa rautatiepalveluissa suur-Lontoon alueella.

Oyster-kortit perustuivat pitkään Octopus-korteista poiketen NXP/Philipsin Mifare-standardiin, mutta vuoden 2009 lopussa kaikki uudet Oyster-kortit

käyttivät Mifare DESFire -siruja. Vuoden 2010 helmikuusta alkaen vanhoja Mifare-pohjaisia Oyster-kortteja ei enää laskettu liikkeelle. Nykyään myös muualla maailmassa Mifare DESFire -pohjaiset kortit ovat laajasti käytössä julkisen liikenteen älykorttijärjestelmissä. (Balaban 2010d.)

Oyster-kortteja on eri variaatioita ja muun muassa vuonna 2007 Barclays-pankki laski liikkeelle pankki- ja luottokortin, jotka sisälsivät OysterCardin toiminnot eli niin sanotun OnePulse-kortin (Barclaycard 2009). Myös suur-Lontoon alueella asuville yli 60 vuotta täyttäneille sekä invalideille kehitettyyn Freedom Pass -korttiin lisättiin Oyster Card -ominaisuus vuonna 2004. (London Councils 2010.)

Niin kuin uudet maksutavat yleensä, niin myös Oyster Card on saanut käyttäjiltään negatiivista palautetta niin yksilönsuojaan, kortin suunnitteluun kuin myös teknisiin ongelmiin liittyen. Esimerkiksi vuonna 2006 hollantilaiset tutkijat onnistuivat murtamaan Mifare-pohjaisen Oyster-kortin tietoturvaominaisuudet. He skannasivat kortinlukijan hankkiakseen vaadittavan kryptografisen avaimen, jonka avulla he pystyivät rakentamaan kannettavalle tietokoneelle valelukijan. Tietokoneeseen kytkettyä langatonta antennia hyväksikäyttäen he kykenivät lukemaan metrossa olevien matkustajien Oyster-korttien tiedot. Saatuaan tiedot pystyivät he kloonaamaan kortin ja käyttämään kloonattua Oyster-korttia seuraavana päivänä maksuvälineenä. Tämä saattoi toimia ennakkotapauksena, joka vaikutti osaltaan, kun päädyttiin vaihtamaan Mifare-siru uuteen Mifare DESFire-siruun. (Lew 2008.)

Kuva 16. Lontoossa käytössä oleva Oyster Card (Dex 2007).

Luottoyhtiöiden palveluja

Johtavat kansainväliset luottoyhtiöt, kuten Visa, MasterCard ja American Express ovat jo laskeneet käyttöön omat kuvan 17 mukaiset kontaktittomat maksukorttinsa niin Aasiassa, Amerikassa, kuin myös Euroopassa. Pankeista muun muassa Citibank, JPMorgan Chase, Barclays ja HSBC olivat edelläkävijöitä näiden wave & pay -korttien käyttöönotossa.

Kuva 17. Luottoyhtiöiden RFID-pohjaiset maksukortit.

MasterCard oli ensimmäinen luottoyhtiö, joka julkaisi kontaktittoman PayPass maksukorttinsa vuonna 2003. Kyseessä oli tuolloin ainoastaan 9 kuukauden pilottijakso, joka toteutettiin yhteistyössä muutaman pankin kanssa. Pilottiin osallistui yli 16 000 käyttäjää ja enemmän kuin 60 kauppiasta. Vuonna 2005 MasterCard otti PayPass-kortit vakituiseen käyttöön tietyillä aloilla ja syyskuussa 2008 PayPass oli saatavissa jo noin 30 suuresta pankista. Kesäkuussa 2010 liikkeelle on laskettu maailmanlaajuisesti arviolta 78 miljoonaa PayPass-korttia, ja maksutapana se toimi noin 245 000 eri liikkeessä ympäri maailman. Yhdysvaltojen lisäksi MasterCard PayPass on saatavilla 36:ssa eri maassa, mutta Suomi ei kuitenkaan mahdu listalle. PayPass-kortilla voidaan suorittaa ilman PIN-koodia alle $50:n ostoksia mutta ostorajat ovat maakohtaiset, koska esimerkiksi Iso-Britanniassa rajana on £10 ja Saksassa 25 €. (MasterCard 2010.)

Visa esitteli oman PayWave -RFID-korttinsa syyskuussa 2007. Vuoden 2010 alussa Euroopassa oli laskettu käyttöön yli 6 miljoonaa PayWave-korttia, ja luvun on arvioitu kaksinkertaistuvan vuoden loppuun mennessä. Visan projekti kulkee pahasti kilpailija MasterCardia jäljessä, mutta uusia kortteja lasketaan

liikkeelle yhä kiihtyvään tahtiin. Suurin osa eurooppalaisista PayWave -kortin käyttäjistä on Iso-Britanniasta. Vuoden 2009 tilastojen mukaan Iso-Britannian jälkeen eniten uutta PayWave-korttia oli laskettu liikkeelle Turkissa ja Puolassa. (VisaEurope 2010b.)

Lontoossa Barclays pankki tarjoaa edellä mainittua OnePulse -yhdistelmäkorttia myös versiona, jossa yhdistyy uusi Visa PayWave ja aikaisemmin mainittu Oyster Card. PayWave -maksutavasta on lanseerattu kolme eri variaatiota: Visa Card, Visa Mini Card ja Visa Micro Tag. Visa Card on aivan kuin perinteinen luottokortti, mutta sisältää myös RFID-tunnisteen, joka mahdollistaa “wave & pay” -tyylisen kaupankäynnin. Visa Mini Card eroaa äskeisestä ainoastaan pienemmän kokonsa turvin, ja Visa Micro Tag edustaa uusinta Visan tarjoamaa tekniikkaa ExxonMobilin Speedpassin kaltaisen avaimenperän muodossa. Yhdysvalloissa PayWave oikeuttaa alle $25:n PIN-koodittomiin ostoksiin ja vastaava ostoraja Iso-Britanniassa on £15. Saksassa voidaan tehdä PIN-kooditta alle 20 €:n ostoksia samoin kuin Suomessa toteutuneessa pilotissa. (Visa 2010.)

Vuonna 2005 yhdysvaltalainen luottokorttiyhtiö American Express julkaisi oman näkemyksensä wave & pay -maksusta laskemalla liikkeelle omat Express Pay -korttinsa 50 osavaltiossa. Kuitenkin projekti lähti käyntiin jo pilottivaiheesta vuonna 2002, josta eteenpäin aina vuoteen 2005 järjestelmiä testailtiin eri ympäristöissä. (ContactlessNews 2005.) Vuoden 2010 alussa suurin osa American Express-korteista oli jo Express Pay -kortteja. Yhdysvalloissa Express Pay -korteilla voidaan suorittaa alle $25:n ostokset syöttämättä PIN-koodia. (American Express 2010.)

NFC julkisessa liikenteessä

Aiemmin mainittujen Octopus ja Oyster Cardin lisäksi löytyy lukuisia julkisen liikenteen ympärille koostuvia palvelukorttijärjestelmiä. Nykyään on osittain jo siirrytty tekniikan toiseen aaltoon eli aletaan maksaa NFC-matkapuhelimella.

Puhelimilla voidaan maksaa jo maailman suurimmissa metro- ja linja-autoverkostoissa. Tekniikka on lähes saavuttanut jo muun muassa New Yorkin, Moskovan, Pietarin, Lontoon ja Pariisin.

CASE: New York & New Jersey

Yhdysvalloissa New Yorkissa käynnistyi kuuden kuukauden pilottijakso vuonna 2006, jossa kaupungin metrossa pystyi maksamaan mobiilisti, käyttäen Nokian 6131 NFC-puhelinta. Pilotissa heilautettiin puhelinta lukijan edessä ja MasterCardin PayPass-ominaisuus veloitti maksun kokelailta langattomasti. Pilotissa oli mukana 30 metroasemaa vilkkaan Lexington Avenue -linjan varrelta. (Balaban, 2010b.) Vastaavanlainen kuuden kuukauden pilotti aloitettiin New Yorkissa kesäkuussa 2010 ja se on yhä käynnissä (MasterCard 2010b). Edellisestä pilotista poiketen tässä maksettiin konkreettisilla PayPass ja PayWave -maksukorteilla. Pilotti on laajentunut edeltäjästään siten, että osallistujatahoja on enemmän ja alueellinen toimintasäde on suurempi kattaen muuan muassa New Jerseyn. (MasterCard 2010c; Balaban 2010b.)

CASE: Moskova & Pietari

Vastaavanlaisia pilotteja on ollut ympäri maailman ja muun muassa Moskovassa Venäjän suurin pankki Sberbank julkaisi NFC-pilotin kesäkuussa 2010. Pilotissa olivat mukana kansallinen rautatieverkosto ja Moskovan metro. NFC-puhelimia jaettiin pilottiin osallistuneille kokelaille noin 10 000. Vuoden 2010 viimeisellä neljänneksellä käynnistyy uusi NFC-pilotti, jossa mukana ovat Moskovan metro ja teleoperaattori MTS. Metroasemille on tarkoitus pystyttää niin sanottuja NFC-kioskeja, joista matkustajat voivat hankkia käytössään oleviin matkapuhelimiin eräänlaisen NFC-paketin. Puhelimiin lisätään SIM-kortti + antenni -ratkaisu, jonka avulla voidaan maksaa NFC-tekniikan avulla. (Clark, S. 2010b.) Myös Pietarissa on suunniteltu NFC:n käyttöönottamista maksujärjestelmissä ja pilottijakso alkoikin syyskuun lopulla 2010. Tarkoituksena on saada NFC-maksu kattamaan koko Pietarin julkisen liikenteen sektorin vuoden 2011 aikana. Fyysisesti matkapuhelimissa käytettäisiin microSD-korttia, jossa on low-end Mifare -siru. Hanketta tukee muun muassa

Pietarin Pankki ja Pietarin julkisen liikenteen komitea. Moskovan hankkeesta poiketen pilottiin ei ole osallistunut teleoperaattoreita. Pietarin metroverkostossa kulkee päivittäin yli 6 miljoonaa matkustajaa, joten tahot etsivät varmasti toimivaa järjestelmäntoimittajaa. (Balaban, D. 2010c.)

CASE: Pariisi

Pariisissa on myös ollut käynnissä puolen vuoden mittainen NFC-pilottijakso, jossa matkustajien matkapassit vaihdettiin NFC-passeihin. Pilottiin osallistuu noin 1000 henkeä ja tarkoituksena on, että vuoden 2010 loppuun mennessä kaikissa Pariisin julkisen liikenteen palveluissa voisi maksaa joko käyttäen NFC-puhelinta tai vastaavaa NFC-laitetta tai korttia. (Clark, S. 2010c; 2010d.) Lontoossa Oyster Card -palvelut on tarkoitus laajentaa mobiilisti käytettäviksi vuoden 2011 aikana.

CASE: Deutsche Bahn & BVG

Saksassa on ollut jo vuosia tekniikan ympärillä pyörineitä pilotteja. Yksi suurimmista projekteista on Saksan rautatieoperaattori Deutsche Bahnin Touch&Travel -NFC-liputus (Deutsche Bahn AG 2010). Pilotti tapahtui vuonna 2009 ja mukana oli suuria nimiä, kuten O2, Vodafone ja T-Mobile. NFC-maksuja kokeiltiin Hannoverin ja Frankfurtin välisellä reitillä. Kuitenkin jo vuonna 2008 käynnistyi projekti, johon osallistui 200 kokelasta reitiltä Hannover – Berliini, ja pilotti laajeni 2500 käyttäjään sekä lopulta S-Bahn, U-Bahn ja linja-autoliikenne liittyi kokonaisuudessaan hankkeeseen. Vuoden 2010 alussa osallistujia oli jo yli 3000 ja tarkoituksena on saada NFC-sovellukset kaupalliseen käyttöön vuoden 2011 aikana. (Clark, S. 2010e; 2010f.) BVG eli Berliinin metroverkosto on ilmoittanut suunnitelmistaan ottaa NFC maksutavaksi muiden rinnalle vuoden 2012 alussa. Lisäksi he aikovat samalla uusia kokonaan elektronisen liputuksen palvelut. (Juckel 24.9.2010, sähköpostiviesti.)

Lentoyhtiöillä ei ole vielä tarjota RFID/NFC-maksuja, mutta erilaiset mobiilipalvelut ovat jo yleistyneet, kuten esimerkiksi check-in -palveluita on jo alettu siirtää mobiilimaailmaan. British Airways kertoo, etteivät he vielä tarjoa asiakkailleen NFC-maksuvaihtoehtoa, mutta he korostivat uudistuneita

mobiilipalvelujaan niin iPhone, Blackberry kuin Android -ympäristössä. (British Airways UK 25.9.2010, sähköpostiviesti.) Lisäksi United Airlines, Air France, KLM, Lufthansa ja Finnair olivat yhteydenottolistallamme, eikä mikään yhtiö tarjonnut NFC-pohjaista maksutapaa lipunmyynnissä. Lufthansalla etätunnistustekniikat ovat käytössä tekniikan osastoilla ja niitä käytetään hyväksi muun muassa logistiikassa. Lufthansalla ei kuitenkaan nähdä NFC-tekniikkaa vaihtoehtona lippujen ostossa, koska ensinnäkään lentolippujen osto ei ole come-by-ride-tyylistä toisin kuin metro ja junaliput. Lentoliput ostetaan yleensä kotona tai matkatoimistosta ja näin ollen quick-payment-method ei ole tarpeellinen. Toiseksi todetaan, ettei tietokoneissa ole ainakaan vielä tarvittavia NFC-lukijoita, joita lentolippujen NFC-etäosto vaatisi. (Sowa 22.10.2010, sähköpostiviesti.)

8 TULEVAISUUDEN NÄKYMÄT

> ”RFID-tekniikka synnyttää Internetin uuden kehitysaallon, jonka tuloksena miljardit älylaitteet ja kehittyneet anturitekniikat yhdistetään maailmanlaajuiseksi viestintäinfrastruktuurien verkoksi” (Dimitriadis 2007).

Tämä Internetin uusi kehitysvaihe on aiemmin mainittu esineiden Internet. RFID-tekniikalla tulee olemaan poliittista merkitystä, siitä voi tulla uusi kasvun ja työllisyyden veturi. (Dimitriadis 2007.) RFID- ja NFC -tekniikka tulee luomaan mahdollisuuden uudenlaiseen automatisoituneempaan maailmaan. RFID-tekniikka tulee tulevaisuudessa yleistymään niin yritysten kuin kuluttajienkin käytössä. Yritykset käyttävät tätä tekniikkaa aiemmin mainitusti logistiikassa, mutta se tulee myös olemaan osana laadunvarmistusta ja riskienhallintaa. Osa yritysten käytössä olevista RFID/NFC-järjestelmistä on osana myös kuluttajien elämää, kuten esimerkiksi postin tilausseuranta ja lentokentillä toimiva matkatavaroiden seurantajärjestelmä. Kuluttajille tekniikka tuo kontaktittomat maksutavat, innovatiiviset kodinkoneet ja helppokäyttöisyyttä henkilökohtaiseen tietojenkäsittelyyn.

Tahvanainen ja Tarkka ovat kirjoittaneet (liite1) fiktiivisiä tarinoita tulevaisuuden perhe-elämästä. Joitakin Tahvanaisen ja Tarkan ajatukset voivat hieman

pelottaa. Me uskomme, että tarinat voivat toteutua kymmenen vuoden sisällä. Tällainen helpottaisi myös erityisryhmiä normaalissa elämässä. Olisi hienoa, jos esimerkiksi NFC-puhelimella voisi hallita valoja, sähkölaitteita ja vaikkapa hissien toimintaa. Käynnissä olevan FinnCity2-hankkeen perusteella voidaan todeta, että etätunnistustekniikka tulee laajenemaan aiemmin todettujen julkisen sektorien tarjoamista palveluista kohti mobiilimaksamista.

Omien tutkimuksiemme perusteella meille on tullut mielikuva, jossa Aasia ja Kaukoitä nousevat maailman edistyneimmäksi teknologia- ja talousmahdeiksi. European-American Business Councilin toimitusjohtaja Michael C. Maibach arvioi myös Euroopan ja Amerikan menettävän innovaatioetunsa Aasialle, eritoten Singaporelle ja Kiinalle (Schindler 2009, 4). Länsimaat ovat tähän asti käyttäneet Aasian halvan työvoiman maita omien innovaatioidensa valmistajina. Sen seurauksena aasialaiset ovat saaneet runsaasti tietotaitoa, joka edesauttaa heidän mahdollisuuksiaan alkaa itse suunnitella uusia innovaatioita. Tämä tulee näkymään eritoten erilaisten elektronisten laitteiden tuotekehityksen siirtymisessä Aasian maihin.

Tämän skenaarion torjumisen elinehto on länsimaiden kilpailukyvyn säilyttäminen, mikä vaatii teknologioiden innovatiivisessa kehityksessä mukana pysymistä. RFID on osa mainittua innovatiivista kehitystä ja RFID-tekniikan menestyminen vaatii yrityksiltä kykyä todistaa kuluttajille tekniikan tuomat hyödyt. Yritysten tulisi siis vedota ihmisten tunteisiin muun muassa korostamalla RFID:n mahdollisuuksia toteuttaa luotettavampaa terveydenhuoltopalvelua sekä älykkäämpää kierrätystä. (Schindler 2009, 4.) Suomessa on jo kokeiltu RFID-tekniikan soveltamista terveydenhuoltoalalla, kun Medixine Oy toteutti kotisairaanhoitopalvelun Imatralla hyödyntäen RFID-tekniikkaa.

Suomalainen tunnistevalmistaja UPM Raflatac on ennustanut kasvua Kaakkois-Aasian markkinoilla (Culha 2010; Ylipoti 2010). Vuonna 2006 isobritannialainen konsulttiyritys IDTechEx arvioi tunnisteiden hintojen putoavan jopa yhden sentin tasolle, jos tunnisteet kyetään painamaan suoraan tuotteeseen tai tuotepakkaukseen. Tämä vaatisi kuitenkin noin triljoonan tunnisteen tilausvolyymin toteutumista. (Paukku, J 2007.)

Odin Technologisin arvioiden mukaan yhdysvaltalainen tunnistevalmistaja Avery Dennison myy noin miljardi RFID-tunnistetta vuonna 2011, mikä on huomattavasti enemmän kuin taantumavuosina 2008 ja 2009. (ODIN Technologies 2010b.) Yhdysvaltain kauppaministeriön johtaja Robin Laytonin mielestä RFID/NFC-tekniikalla on merkittävä rooli maan yritysten talousahdingosta nousussa. Hän korostaa myös innovaatiotekniikan osuutta globaalin talouden kasvussa.(Schindler 2009, 4-5.) On mahdollista, että tulevaisuudessa RFID-tunniste lisätään kaikkiin tehtaissa valmistettuihin tuotteisiin aina lyijykynistä paperikoneisiin. Yksi merkittävimmistä hyödyistä logistisen toiminnan helpottamisen rinnalla on erilaisten väärennösten ja laittomien kopioiden helpompi tunnistus.

Noin 60 % lääkeyhtiöistä käyttää RFID-tunnisteita jo jossain määrin valmistusketjuissa ja tulevaisuudessa kaikki lääkepakkaukset merkitään tunnisteilla väärennösten tunnistamisen helpottamiseksi. (ODIN Technologies 2010.) Nykyään yhä useammat tilaavat Internetistä hyväuskoisina halpoja lääkevalmisteita, jotka saattavat olla hyvin vaarallisia terveydelle. (Poliisi-tv 28.10.2010.) Uskomme, että tulevaisuudessa kyetään kitkemään laitonta lääkekauppaa tutkimamme tekniikan avulla.

RFID/NFC-sovellusten hitaaseen yleistymiseen vaikuttaa eritoten järjestelmien korkea hintataso sekä epätietoisuus ja skeptisyys niiden takaisinmaksuajoista. Vuosien 2008 ja 2009 lama jarrutti tunnisteiden hintojen laskua, minkä takia myyntivolyymit laskivat. ODIN Technologisin toimitusjohtaja Patrik J. Sweeneyn mukaan nykyinen RFID/NFC-järjestelmä kehittyy siten, että järjestelmästä poistuu kokonaan väliohjelmisto eli middleware. Lukijat siis kommunikoisivat suoraan taustajärjestelmässä olevan toiminnanohjausjärjestelmän (ERP) kanssa. Tämä alentaisi varmasti järjestelmien käyttöönotto- ja ylläpitokustannuksia. Nopeammin RFID-tekniikka kuitenkin kasvaa logistiikassa ja terveydenhuoltoalalla. On todennäköistä, että muutaman vuoden sisällä maailmanlaajuiseen suosioon yltää 4-6 kuluttajille suunnattua RFID/NFC -pohjaista sovellusta. On arvioitu, että elektroiikkajätti Applen seuraava versio

iPhone älypuhelimesta sisältäisi UHF-taajuudella toimivan NFC-tunnistusominaisuuden. (ODIN Technologies 2010a.)

Finavia rakennutti 2009 Helsinki-Vantaan lentoasemalle RFID-tekniikkaa hyödyntävän matkatavaroidenkäsittelyjärjestelmän (baggage tracking). Jokaiseen matkalaukun tunnistetarraan on upotettu RFID-tunniste. Tämän ansiosta matkatavaroiden lajitteleminen ja jäljittäminen on nopeutunut Helsinki-Vantaalla huomattavasti. Tietojärjestelmistä pystyy seuraamaan reaaliaikaisesti laukkujen sijainnin. Finavian tutkimuksen mukaan noin 87 % vuoden 2009 matkustajista saivat matkatavaransa alle 30 minuutissa lennon laskeutumisesta Helsinki-Vantaalle. Helsinki-Vantaan matkatavaralajittelujärjestelmä kykenee lajittelemaan noin 7000 laukkua tunnissa. (Finavia 2009, 37.) Vastaavien järjestelmien yleistyminen maailman lentokentille on alkanut.

Matkatavaralajittelujärjestelmää suunniteltaessa on kiinnitettävä huomiota järjestelmän tietoturva-aukkojen minimoimiseen. Rieback ym. esittävät RFID-Virus.org Internetsivustollaan fiktiivisen kuvaelman, miten RFID-tekniikkaan pohjautuvaan järjestelmään on mahdollista tartuttaa virus matkalaukkutunnistetarran avulla. Tämä tunniste tartuttaisi viruksen järjestelmän tietokantaan. Myös kaikki järjestelmän läpi kulkevat laukut saisivat täten tartunnan ja levittäisivät sitä eteenpäin muiden lentokenttien tavaranlajittelujärjestelmiin. (Rieback ym. 2006.) Kuvaelman käydessä toteen olisi maailmanlaajuinen kaaos valmis. Skenaarion toteutuminen loisi huumesalakuljettajille ja muille kriminaaleille otollisen ympäristön toimilleen.

Kotitalouksia ajatellen suurin ja lähimpänä tulevaisuutta oleva askel tulee olemaan jo aiemmin mainitut NFC-pohjaiset maksutavat. NFC-puhelimella toimivasta maksujärjestelmästä on jo nyt tehty Suomessa onnistuneita pilottihankkeita. Vaikuttaa siltä, että järjestelmä olisi jo valmis siirrettäväksi tuotteistamisvaiheeseen. Viime vuosina kaupat ovat kuitenkin joutuneet tekemään suuria laite- ja ohjelmistoinvestointeja, kun perinteisistä pankki- ja luottokorteista ollaan siirtymässä sirukortti-maksamiseen. Tällä hetkellä ollaan tilanteessa, jossa yhä useammissa paikoissa on mahdollista maksaa sirukortilla. Suurten investointien jälkeen ei ole ehkä halua siirtyä heti seuraavan

sukupolven NFC-maksuihin, koska se tulisi olemaan kallista. Uskomme kuitenkin sirukorttien olevan jonkinlainen välivaihe maksamisessa, ja ennen pitkää siirryttäisiin kohti kontaktittomia maksutapoja. Ensin olisi vuorossa kontaktittomien maksutapojen tuleminen nykyisten tapojen rinnalle, ja hiljalleen perinteiset magneettinauhakortit poistuisivat käytöstä. Uskomme jopa sirukorttien käytön vähenemiseen ja mahdollisuuteen niiden poistumiseen kokonaan pois markkinoilta. Käteistä valuuttaa RFID/NFC-tekniikka ei kuitenkaan ole syöksemästä pois käytöstä.

Teoriassa tulevaisuudessa on mahdollista, että sinulla on vain yksi ainut kortti lompakossasi. Tämä kortti voisi olla yhtä aikaa pankki-, luotto-, kirjasto-, joukkoliikenne-, kuntosali- ja kaupunkikorttisi, sekä koti- ja työavaimesi. Biometrinen sormenjälkitunnistus voisi olla hyvä tapa korttitapahtumien varmentamiseksi. Ennen järjestelmän käyttöönottamista on ratkaistava muutamia tietoturvaongelmia: Mitä jos kortti hukkuu? Onnistuuko kortin mitätöiminen helposti? Mielestämme nämä asiat ovat yksinkertaisesti ratkaistavissa. Käyttäjäkunta voi kuitenkin tuntea turvattomuutta miettiessään edellä mainittuja asioita. Syynä pelkoon saattaa olla se, että kortti olisi liitettynä pankkitietoihin, vaikka sitä ominaisuutta ei aina käytettäisikään.

9 JOHTOPÄÄTÖKSET

Tutkimuksemme päämääränä oli tutkia etätunnistustekniikkojen tämän hetken tilannetta kuluttajien jokapäiväisessä elämässä niin Suomessa kuin ulkomaillakin. Teoreettisessa osuudessa käytimme pääasiassa ulkomaalaisia teoksia suomalaisen aineiston vähäisyydestä johtuen. Saimme mielestämme kokoon järkevän kokonaisuuden tekniikoiden perusteista. Käytännön tutkimusta alan tämän hetken tilanteesta teimme suuremmaksi osaksi etsimällä Internetistä erilaista aineistoa. Lähetimme myös sähköpostilla kyselyjä eri puolilla maailmaa sijaitseviin joukkoliikenneverkostoihin saadaksemme heidän järjestelmistään yleisiä tietoja. Sähköpostien lähetysmäärään verrattuna saimme vastauksia harmillisen vähän.

Tutkimuksessa esiin tulleet tekniikat tulevat olemaan näkyvä osa tulevaisuuden maailmaamme ja siksi aihe on enemmän kuin ajankohtainen. Tekniikasta on jo nyt paljon tietoa ja kohta on täyden tuotteistamisen aika käsillä. Emme ennen kevättä 2010 tienneet aiheesta juuri mitään ja siksi tartuimmekin haasteeseen ja se osoittautui hyvin mielenkiintoiseksi.

Näemme tekniikan hitaaseen yleistymiseen syinä muun muassa sen, että kuluttajat eivät ole valmiita suuriin muutoksiin, koska pelkäävät uuden tekniikan tuomia haasteita. Ihmiset ovat luonteeltaan epäileväisiä ja tekniikoista puheen ollen ajoittain hyvinkin skeptisiä. Se, miten kuluttajat saataisiin tekniikan taakse, onkin kysymys erikseen. Se, että tietotaito on alan osaajilla, sekä mahdollisesti niiden yritysten sisällä, jotka järjestelmiä käyttävät tai harkitsevat niiden käyttöönottoa, ei riitä tuomaan luottamusta kuluttajien piiriin. Vaadittaisiin jokin tapa saada tieto kuluttajille, jolloin asenteet ja mielikuvat saattaisivat muuttua. Jotta voidaan antaa kuluttajille rehellinen kuva tietoturvallisista järjestelmistä, on asian parissa tehtävä jatkuvasti kehitystyötä. Tietoturvan parantamisessa on standardijärjestöillä hyvin suuri vaikutus, koska käytäntöjen yhdistäminen niin, että kaikkialla olisi käytössä samat tietoturvamäärittelyt, loisi erityisen toimivan kokonaisuuden.

Tutkimuksen aikana olemme saaneet hyviä ja vaikuttavia kontakteja. Näemme onnistuneen verkostoitumisen auttaneen huomattavasti työskentelyä, ja mielipiteiden jakaminen auttaa luomaan eheän ja luotettavan kokonaiskuvan aiheesta. On perin selvää, että asioista saa luotettavamman kuvan, kun tekstissä on mukana suurten ja vaikutusvaltaisten elinten kommentteja ja näkemyksiä. Jouduimme kuitenkin huomaamaan, että suomalaisten kontaktien luominen aiheeseen liittyen oli haastavaa ja lähes turhauttavaa. Vastapainoksi ulkomaisilta tahoilta apua saatiin kiitettävästi. Jouduimme kuitenkin sen ongelman eteen, jossa eri tahot olivatkin eri mieltä asioista. Toki mielipiteitä voi olla erilaisia, mutta kun faktatiedoistakin saa erilaisia näkemyksiä, on hämmennys suuri. Haasteellisuus piileekin siinä, miten valita oikeat tiedot ja kehen voi luottaa.

LÄHTEET

American Express 2010. How Does expresspay Work? Viitattu 3.11.2010 https://www217.americanexpress.com/cards/loyalty.do?page=expresspay&module=2

Association for Automatic Identification and Mobility 2010. RFID Glossary of Terms. Viitattu 2.9.2010 http://www.aimglobal.org/technologies/rfid/rfid_Glossary.asp

Balaban, D. 2010a. NFC on Campus: UK Pilot is a Possible Prelude To College Launch. NFC Times 14.6.2010 http://www.nfctimes.com/news/nfc-campus-uk-pilot-possible-prelude-collegewide-launch

Balaban, D. 2010b. New York Extends Trial of Open-Loop Fare Payment. NFC Times 14.5.2010 http://www.nfctimes.com/news/new-york-extends-trial-open-loop-fare-payment

Balaban, D. 2010c. St. Petersburg Metro to Trial Contactless-Mobile Ticketing. NFC Times 27.9.2010 http://www.nfctimes.com/news/st-petersburg-metro-trial-contactless-mobile-ticketing

Balaban, D. 2010d. Transport for London to Discard Mifare Classic. NFC Times 21.1.2010 http://www.nfctimes.com/news/transport-london-discard-mifare-classic-seeks-desfire-sims

Banks, J; Hanny, D; Pachano, M & Thompson, L. 2007. RFID Applied. Hoboken, New Jersey: John Wiley & Sons, Inc.

Barclaycard 2009. Barclaycard OnePulse FAQs. Viitattu 4.11.2010 http://www.barclaycard-onepulse.co.uk/onePulseFaq.html.

Bhatt, H. & Glover, B. 2006. RFID Essentials. 1. painos. Sebastopol: O'Reilly Media, Inc.

Bhutani, M & Moradpour, S. 2005. RFID Field Guide, Deploying Radio Frequency Identification Systems. Santa Clara, California: Sun Microsystems Press.

Boslau, M & Lietke, B 2005. RFID is in the Eye of the Consumer – survey results and implications. Institute for marketing and retailing, University of Göttingen, Germany. Viitattu 3.11.2010 http://www.uni-goettingen.de/de/document/download/36d43508d0b9a98373dbb69164425779.pdf/athen_vortrag.pdf

Ciruela, S; Delgado, M; & Marin, N. 2010. A Ubiquitous Intelligent Tutoring System for Aiding Electronic Learning. Teoksessa Setchi, R; Jordanov, I & Jain, L. (toim.) Knowledge-Based and Intelligent Information and Engineering Systems: 14th international Conference, KES 2010 (Cardiff, UK, September 2010. Proceedings, Part IV) Berlin: Springer-Verlag, 70-79

Clark, S. 2010a. Paris transport operators begin NFC ticketing trial. Near Field Communications World. 11.2.2010 http://www.nearfieldcommunicationsworld.com/2010/02/11/32680/paris-transport-operators-begin-nfc-ticketing-trial/

Clark, S. 2010b. Moscow Metro and MTS to launch NFC ticketing service in Q4 2010. Near Field Communications World. 23.6.2010 http://www.nearfieldcommunicationsworld.com/2010/06/23/34014/moscow-metro-and-mts-to-launch-nfc-ticketing-service-in-q4-2010/

Clark, S. 2010c. Paris transport operators to launch NFC ticketing from the end of 2010. Near Field Communications World. 16.6.2009 http://www.nearfieldcommunicationsworld.com/2009/06/16/31330/paris-transport-operators-to-launch-nfc-ticketing-from-the-end-of-2010/

Clark, S. 2010d. Paris transport operators begin NFC ticketing trial. Near Field Communications World. 11.2.2010 http://www.nearfieldcommunicationsworld.com/2010/02/11/32680/paris-transport-operators-begin-nfc-ticketing-trial/

Clark, S. 2010e. Telefónica O2 joins Deutsche Bahn's NFC ticketing project. Near Field Communications World. 19.8.2009 http://www.nearfieldcommunicationsworld.com/2009/08/19/31527/telefonica-o2-joins-deutsche-bahns-nfc-ticketing-project/

Clark, S. 2010f. Deutsche Bahn opens registration for next phase of NFC ticketing project. Near Field Communications World. 5.10.2009 http://www.nearfieldcommunicationsworld.com/2009/10/05/31873/deutsche-bahn-opens-registration-for-next-phase-of-nfc-ticketing-project/

Culha, N. 2010. Service diverce markets. Raflatalk Express Asia Pacific 7/2010, 2. Viitattu 1.11.10 http://www.upmraflatac.com/asia/eng/images/55_80313.pdf

Deutsche Bahn AG 2010. Touch and Travel - Infos zum Piloten. Viitattu 2.11.2010 http://www.touchandtravel.de/site/touchandtravel/de/infos__piloten/infos__piloten.html

Dex, R. 2007. Oyster card bus and tram fares cut by 10p. London Evening Standard 1.10.2007 http://www.thisislondon.co.uk/standard/article-23414489-oyster-card-bus-and-tram-fares-cut-by-10p.do

Dimitriadis, D. 2007. Euroopan talous- ja sosiaalikomitean lausunto aiheesta: "Radiotaajuustunnistus (RFID)". Euroopan unionin virallinen lehti 27.10.2007. Viitattu 24.10.2010 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:256:0066:0066:FI:PDF

eGov 2010. Check on travel document counterfeit - eGov - Articles - Cover Story. Viitattu 2.11.2010 http://www.egovonline.net/articles-list/45-cover-story/3958-check-on-travel-document-counterfeit.html

Ekström, S. 2001. RFID – Mitä lyhenne tarkoittaa? Viitattu 14.10.2010 http://www.exxi.fi/files/file/esitteet/RFIDexxi.pdf

ExxonMobil 2010. Welcome to Speedpass. Viitattu 2.11.2010 http://www.exxonmobil.com/ap-english/speedpass.aspx

EUR-Lex 2007. EUR-Lex – 52007DC009. Viitattu 13.10.2010 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0096:FIN:FI:HTML

Finavia 2009. Matkoja – Maisemia. Finavian vuosikertomus 2009. Viitattu 28.10.2010 http://www.finavia.fi/files/finavia2/vuosikertomukset_pdf/42670_FINAVIA_vsk_FI.pdf

Finkenzeller, K. 2003. RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification. 2. painos. Hoboken, New Jersey: John Wiley & Sons, Inc.

Garfinkel, S. & Rosenberg, B. 2005. RFID: applications, security, and privacy. 1. painos. New York: Addison-Wesley

Helsingin seudun kauppakamari 2010. TURVALLISUUSOPAS - Viranomaisten turvallisuustoiminta kuntien ja yritysten näkökulmasta. Viitattu 4.11.2010 http://www.helsinki.chamber.fi/files/1027/Turvallisuusopas.pdf

Henkilötietolaki 22.4.1999/523

Hitachi 2010. The World's smallest RFID IC. Viitattu 1.8.2010 http://www.hitachi.co.jp/Prod/mu-chip/

Honkanen, M.; Jalo, J. & Kalliokoski, S 2009. Nestekaasupullojen RFID-avusteinen tilaus-toimitusketjujen hallinta. Viitattu 1.6.2010 http://www.rfidlab.fi/sites/rfidlab.fi/files/kaasuRFID_loppuraportti_08_10_2009.pdf

Hospitality.net 2008. TeliaSonera and VingCard (ASSA ABLOY Group) demonstrate hotel room access using an NFC mobile phone and lock. Viitattu 12.9.2010 http://www.hospitalitynet.org/news/4038612.search?query=abloy+nfc

HSL Helsingin seudun liikenne 2010. HSL Helsingin seudun liikenne – Kortin käyttö. Viitattu 18.10.2010 http://www.hsl.fi/FI/matkustajanopas/matkakortti/Sivut/matkakortinkaytto.aspx

Hunt, V.D; Puglia, A. & Puglia, M. 2007. RFID: A guide to radio frequency identification. Hoboken, New Jersey: John Wiley & Sons, Inc.

Järvinen, M 2007. Epäilyttääkö etäluku? Systeemityö 1/2007, 21-22

Kleiner, K. 2005. Metal shields and encryption for US passports. New Scientist 28.10.2005 http://www.newscientist.com/article/dn8227-metal-shields-and-encryption-for-us-passports.html

Korkimo, A. 2008. Passien rfid-sirut murrettiin. Elektroniset passit ja matkakortit joutuvat roskiin? Tietokone 12.8.2008. Viitattu 21.10.2010 http://www.tietokone.fi/uutiset/2008/passien_rfid_sirut_murrettiin

Kranenburg, R. & Ward, M 2006. RFID: Frequency, standards, adoption and innovation. Viitattu 12.7.2010 http://www.jisc.ac.uk/media/documents/techwatch/tsw0602.pdf

Kuluttajansuojalaki 20.1.1978/38

Kärkkäinen, K. 2006. RFID-logistiikassa. Viitattu 1.9.2010 http://www.lrg.tkk.fi/publications/RFID_logistiikassa_010806.pdf

Laki yksityisyyden suojasta työelämässä 13.8.2004/759

Lew, A 2008. Hackers Crack London Tube's Ticketing System. Autopia 24.6.2010. Viitattu 4.11.2010 http://www.wired.com/autopia/2008/06/hackers-crack-l/

London Councils 2010. How to use your Freedom Pass. Viitattu 4.11.2010 http://www.londoncouncils.gov.uk/freedompass/howto/

MasterCard 2010a. Mastercard PayPass - Paypass Performance Insights. Viitattu 25.10.2010 http://www.paypass.com/performance_insights.html

MasterCard 2010b. New Jersey and New York Transit Agencies Partner with MasterCard on Tap & Go™ Payment System to Enhance Commuter Experience. Viitattu 2.11.2010 http://mastercard.presslift.com/ridenynj

MasterCard 2010c. About the trial. Viitattu 2.11.2010 http://www.ridenewyorknewjersey.com/about.html

Mazo, A. Near Field Communication Application Provisioning Framework. Pro gradu. Tietojenkäsittelytiede. Luleå: Luleå University of Technology. Saatavissa myös: http://epubl.ltu.se/1402-1781/2010/003/LTU-CDUPP-10003-SE.pdf

NFC Forum 2010a. NFC Forum: Members. Viitattu 13.6.2010 http://www.nfc-forum.org/member_companies/

NFC Forum 2010b. NFC Forum: Specifications. Viitattu 13.6.2010 http://www.nfc-forum.org/specs

NFC Forum 2010c. NFC Forum : Frequently Asked Questions. Viitattu 1.11.2010 http://www.nfc-forum.org/resources/faqs#headConsumers

Nokia 2010. Nokia 6131. Nokia – Devices. Viitattu 15.8.2010 http://www.forum.nokia.com/Devices/Device_specifications/6131_NFC/6131_NFC_main.jpg

Nurminen, T. 2005. Suomen teollisuus jää rfid-junasta. Talouselämä 16.3.2005. Viitattu 1.1.2010 http://www.talouselama.fi/kolumni/article165441.ece

Octopus 2007. Octopus Holdings Limited - Press Releases. Viitattu 2.11.2010 http://www.octopus.com.hk/release/detail/en/20070913.jsp

ODIN 2010a. ODIN 2010 RFID Predictions Video- ODIN rfid software and solutions. Viitattu 29.10.2010 http://www.odintechnologies.com/index.php?option=com_content&view=article&id=254

ODIN 2010b. Avery Dennison to sell one billion RFID tags in 2011? Viitattu 29.10.2010 http://blog.odintechnologies.com/odin-rfid-blog/bid/52715/Avery-Dennison-to-sell-one-billion-RFID-tags-in-2011

Oulun kaupunki 2010. Suunnitelman kortti. Viitattu 10.10.2010 http://www.ouka.fi/kehittamishankkeet/kehittamisohjelmat/hankekortit/Hankekortti.asp?ID=519

Paukku, J. 2007. Painaminen suoraan pakkaukseen pudottaisi RFID tunnisteen hinnan sentteihin. GT-lehti 1/2007.

Paus, A. 2007. Near Field Communications in Cell Phones. Seminaarityö. Bochum: Ruhrin yliopisto. Saatavilla myös http://www.crypto.rub.de/imperia/md/content/seminare/itsss07/near_field_communication_in_cell_phones.pdf

Philips 2002. Mifare® Standard 4 kByte card IC MF1 IC S70 Functional specification. Viitattu 1.9.2010 http://www.nxp.com/acrobat_download2/other/identification/m043531.pdf

Philips 2008. Mifare DESFire 4K White PVC Cards. Viitattu 25.10.2010 http://mifare.net/downloads/MIFARE%20DESFire%20EV1_HR_FINAL%20VERSION.pdf

Poliisi 2010a. Passi. Viitattu 19.10.2010 http://www.poliisi.fi/poliisi/home.nsf/pages/0F1952F245FE4200C22571CE004C0912?opendocument

Poliisi 2010b. Passin mikrosirun toimintaperiaatteet. Viitattu 19.10.2010 http://www.poliisi.fi/poliisi/home.nsf/pages/93A9A0F1F84CD0A9C225717E0045AC7E?opendocument

Poliisi-tv, 28.10.2010. Esitetty 28.10.2010 YLE2.

Rieback, M; Simpson, P; Crispo, B & Tanenbaum, A 2006. RFID Viruses and Worms. Viitattu 4.11.2010 http://www.rfidvirus.org/

RFID in Europe 2009. Frequently Asked Questions. Viitattu 24.10.2010 http://www.race-networkrfid.eu/faq#1

RFID Journal 2010. Genesis of the Versatile RFID Tag. Viitattu 12.7.2010 http://www.rfidjournal.com/article/view/392/1/2

RFID Lab Finland 2010. RFID-standardit. Viitattu 24.10.2010 http://www.rfidlab.fi/rfid-standardit

Scher, B 2004. Understanding RFID Frequencies. Viitattu 3.6.2010 http://rfidusa.com/superstore/pdf/Understanding_RFID_Frequencies.pdf

Shindler, R. 2009. 2nd Transatlantic Symposium on the Societal Benefits of RFID Brussels, Belgium May 6th 2009 - Symposium report. Brussels:RAND Europe. Saatavissa http://ec.europa.eu/information_society/policy/rfid/documents/euus_symposiumreport.pdf

Seppä, H. 2009. Vallankumouksellinen RFID: Etätunnistusteknologian kehitys meillä ja maailmalla. Tekesin katsaus 249/2009. Helsinki: Tekes. Saatavissa myös http:// www.tekes.fi/fi/document/27018/rfid_pdf.pdf

Sisäministeriö 2010. Biometriahanke – Biometrinen passi. Viitattu 19.10.2010. http://www.intermin.fi/intermin/hankkeet/biometria/home.nsf/pages/596EE8B62C0D31ABC2256E52002ED3F6

Sweeney II, P. 2005. RFID for Dummies. Indianapolis: Wiley Publishing, Inc.

Sähköisen viestinnän tietosuojalaki 16.6.2004/516

Tahvanainen, M & Tarkka, K 2007. RFID muuttaa varastosta kotiin. Systeemityö1/2007, 23-25

Tampereen kaupunki 2005. eTampere-kortti Loppuraportti versio 5.2 / 6.4.2005. Viitattu 20.10.2010 http://www.tampereenseutu.fi/@Bin/1553095/etampere_loppuraportti_ako.rtf

ToP Tunniste 2006. Identified by ToP Tunniste: RFID-tekniikka. Viitattu 2.9.2010 http://www.toptunniste.fi/index.php?id=rfid-lukija-antenni-tunniste&L=3%2F%2Fassets%2Fsnippets%2Freflect%2Fsnippet.reflect.php%3Freflect_base%3D

Turku 2010. www.turku.fi >> turku.fi >> Kartat, kadut ja liikenne >> Liikenne >> Bussit ja aikataulut >> Lippulajit ja hinnat >> Bussikortit. Viitattu 1.11.2010 http://www.turku.fi/Public/default.aspx?nodeid=11922&culture=fi-FI&contentlan=1

United States Government Accountability Office 2005. Report to Congressional Requesters: INFORMATION SECURITY – Radio Frequency Identification Technology in the Federal Government. Viitattu 2.11.2010 http://epic.org/privacy/surveillance/spotlight/0806/gao05551.pdf

Vaalisto, H 2010. Tukholmalaishotelli korvaa huoneen avaimen kännykällä. IT-Viikko 2.11.2010. Viitattu 4.11.2010 http://www.itviikko.fi/ratkaisut/2010/11/02/tukholmalaishotelli-korvaa-huoneen-avaimen-kannykalla/201015239/7

Viestintävirasto 2009. Viestintävirasto – Tietoturva ja –suoja. Viitattu 24.10.2010 http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva.html

Visa 2010. Visa payWave | Personal | Visa USA. Viitattu 25.10.2010 http://usa.visa.com/personal/cards/paywave/index.html

Visa Europe 2010a. Visa mobile. Viitattu 15.6.2010 http://www.visaeurope.com/en/site_services/idoc.ashx?docid=d8add4d0-1330-46c7-be33-ff50cee56857&version=-1

VisaEurope2010b. Visa PayWave. Viitattu 25.10.2010 http://www.visaeurope.com/en/about_us/innovation/visa_paywave.aspx

Want, R 2004. RFID A Key To Automating Everything. Scientific America 1/2004,59. Viitattu 25.10.2010 http://www.eknigu.com/get/P_Physics/PPop_Popular-level/Scientific%20American%20January%202004(97s).pdf

Ward, M 2006. RFID: Frequency, standards, adoption and innovation. Viitattu 12.7.2010 http://www.jisc.ac.uk/media/documents/techwatch/tsw0602.pdf

Ylipoti, I. 2010. Rising to the challenge in the Asia-Pacific. Raflatalk Express Asia Pacific 7/2010,1.Viitattu 1.11.2010 http://www.upmraflatac.com/asia/eng/images/55_80313.pdf

ZEBRA Technologies 2010. RFID Tag Characteristics. Viitattu 13.9.2010 http://www.zebra.com/id/zebra/na/en/index/rfid/faqs/rfid_tag_characteristics.html

LIITE 1 RFID muuttaa varastosta kotiin

RFID-sovellukset voisivat hyvin olla osa arkeamme jo nyt. Teknisesti se olisi mahdollista. Maailma ei vain ole ajatukselle vielä kypsä. Muutaman sentin hintainen yksittäinen RFID-siru ei ole enää ainakaan kustannuskysymys.

Yksilönsuojasta on RFID-sirujen kanssa huolehdittava. Äärimmäisyyksiin vietynä yksilönsuojan korostaminen rajoittaa kuitenkin kehitystyötä merkittävästi. Isoveljen valvontaa ei varmasti kukaan halua lisää eikä vastasyntyneille lapsille tulevaisuuden Suomessakaan asenneta sci-fi-elokuvista tutulla tavalla RFID-sirua takaraivoon. Ei ainakaan vastoin heidän tai vanhempiensa tahtoa. Jos käyttäjä itse hyväksyy RFID-teknologian hyödyntämisen, niin sen pitäisi riittää hyväksynnäksi myös lainsäätäjälle.

Miltä tulevaisuuden arki näyttää RFID-sirujen näkökulmasta? Seuraavat kolme tarinaa kertovat tulevaisuuden koululaisen, tietotyöläisen ja seniorikansalaisen elämästä RFID-maailman keskellä.

Vilma 16 v: Koululaisen reput ja pelivehkeet vihdoinkin tallessa

Vilma, 16-vuotta, herää aamulla kotoaan. Hetki vetelehtimistä sängyssä, vaatteet päälle ja kylpyhuoneeseen. Vilman paidannapissa oleva RFID-siru kertoo talon tietojärjestelmälle missä tyttö milloinkin liikkuu, jolloin valot syttyvät ja sammuvat tarpeen mukaan. Kylpyhuoneessa Vilmaa odottaa vaaka, joka tunnistaa tytön. Paino on pudonnut muutaman gramman eilisestä, joten Vilma päättää syödä aamiaiseksi suklaavanukkaan. Vaaka mittaa myös rasvaprosentin eikä koneella ole siitä mitään huomautettavaa. Aamiaisen jälkeen Vilman koulureppu vilauttaa repun läpässä olevaa vihreää valoa, kun kaikki sinä päivänä tarvittavat koulukirjat ovat repussa. Kassi olalle ja bussiin. Bussin tietojärjestelmä kuittaa Vilman bussin käyttäjäksi. Erillisiä matkakortteja ei tarvita.

Apua allergioihin

Koulurakennukseen saapuessaan koulun tietojärjestelmä noteeraa Vilman saapumisen koulun tiloihin ja omaan luokkaansa. Saapumisesta lähtee myös tieto kodin tietojärjestelmään. Vilma on siis päässyt turvallisesti perille. Ensimmäisen tunnin historiankokeessa RFID-nappi kertoo opiskelupisteen tietokoneelle, että koevastauksen antaja on Vilma. Vastattuaan kaikkiin koekysymyksiin lähettää Vilma vastauksen sähköisesti opettajalle. Vilma opiskelee kurssimuotoisessa lukiossa, jolloin opetusta on tarjolla eri puolilla koulurakennusta. RFID-siru kertoo koulun tietojärjestelmälle Vilman osallistumisen kullekin kurssille. Ruokailukin hoituu kätevästi, sillä koulun ruokala osaa ottaa huomioon Vilman ruoka-allergiat jo ruokalan ovella. Eipä ole maitosokeria laktoosi-intolerantikon kanaviillokissa.

Salibandya ilman sähläämistä

Koulupäivän jälkeen Vilma poistuu koulurakennuksesta, jolloin koulun tietojärjestelmä kuittaa asian. Koulun portin jälkeen Vilma liikkuu omalla vastuullaan kohti urheilutaloa ja siellä odottavaa salibandyjoukkueen harjoitusta. Talossa on monta salia. Ovella urheilutalon tietojärjestelmä huomaa tytön ja neuvoo häntä menemään salille numero kuusi. Vilma vaihtaa päälleen urheiluvaatteet ja jättää ulkovaatteensa lukittavaan lokerikkoon. Se avautuu vain Vilman RFID-napin läsnäollessa. Urheilut on urheiltu ja Vilma palaa kotiin. Kotiovella talon tietojärjestelmä kertoo Vilmalle, että äiti on jo tullut kotiin. Omaan huoneeseensa astuessaan kodin tietojärjestelmä muistuttaa Vilmaa vielä päivän läksyistä. Tieto kotitehtävistä on siirtynyt kotiin automaattisesti koulusta. Vilma tekee läksyt ja kutsuu parhaan kaverinsa Sannan kotiinsa. Kodin tietojärjestelmä tunnistaa myös Sannan tämän napissa olevasta RFID-sirusta. Illalla kymmenen aikoihin Vilma menee nukkumaan. Paidannapissa oleva RFID-siru pysyy sen sijaan hereillä 24 tuntia vuorokaudessa.

Jarmo 44 v: Työelämää ja elektroniikkaa

Jarmo, 44 vuotta, herää aamulla. Herätyskellossa oleva valo vaihtuu punaisesta vihreään, jolloin Jarmo tietää, että kylpyhuone on perheen tyttären Vilman jälkeen vapaa. Jarmo astuu klinkkerilattialla sijaitsevalle vaa'alle. Jarmon paino on entisestään lisääntynyt eikä kehon rasvaprosenttikaan ole kehuttavampi. Vaaka kehottaa Jarmoa syömään aamiaiseksi kaurapuuroa. Jarmo virnistää vaa'alle, pukeutuu, nappaa keittiöstä kupin kahvia ja istahtaa kotona olevan työpisteensä ääreen. Jarmo on tietotyöläinen, joka tekee työtään niin kotona, autossa, lentokoneessa kuin toimistollaankin. Kodin työpiste tunnistaa Jarmon RFID-sirusta ja yhdistää tietokoneen suoraan Jarmon työnantajan tietojärjestelmään. Jarmon kone on samalla myös yhteydessä kodin tietojärjestelmään. Jälkimmäinen muistuttaa Jarmoa siitä, että aamun kaurapuuro on edelleen syömättä.

Älypitsaa ja RFID-esitteitä

Lounasajan lähestyessä Jarmo tilaa verkon kautta kotiinsa pitsan. Hän on kyllästynyt kuuntelemaan kotijärjestelmän kaurapuuro- ja terveysmuistutuksia kytkemällä ominaisuuden kokonaan pois päältä. Lounasta tilatessaan hän antaa samalla pizzan tuojan RFID-sirulle luvan avata kotinsa ulko-oven, jotta pitsan voi tuoda suoraan keittiön pöydälle. Laskutus tapahtuu automaattisesti Jarmon tililtä. Pitsa toimitetaan älykkäässä ja kierrätettävässä paketissa, joka pitää ruoan lämpimänä. Kodin tietojärjestelmä kertoo Jarmolle, että keittiön pöydällä olevan pitsan pintalämpötila on edelleen 65 astetta. Sama tieto menee myös pitsayrittäjän laatujärjestelmälle. Kunpa kuljettaisivat pitsan lisäksi vielä kylmää oluttakin, haaveilee Jarmo. Iltapäivällä Jarmolla on seminaari, johon hän ajaa autollaan toimistonsa kautta. Auton istuin säätyy automaattisesti juuri Jarmolle sopivaan asentoon hänen autoa lähestyessään. Toimiston parkkihallissa ovi aukeaa automaattisesti, kun toimiston tietojärjestelmä tunnistaa Jarmon ja Jarmon auton. Huomiseksi Jarmo tarvitsee firman uuden brandin mukaiset esitteet. Jarmo tulostaa sopimukset RFID-kirjoittimella älypaperille. Tulostin tunnistaa Jarmon ja tulostaa esitteet automaattisesti hänen määrittämänsä profiilin mukaisiksi. Samalla älykirjoitin rekisteröi Jarmon käyttämän odottelun kirjoittimen äärellä. Hmm, pitäisiköhän meidän hankkia nopeampi printteri, kun tulostamiseen menee noin paljon aikaa, pohtii Jarmon pomo myöhemmin kirjoittimen raporttia tutkiessaan.

Vihdoinkin hyviä tv-ohjelmia

Seminaariin saapuessaan Jarmo pysäköi autonsa seminaaritilan parkkihalliin, joka laskuttaa Jarmoa pysäköinnistä automaattisesti. Seminaari-ilmoittautumiseen ei kulu suurta aikaa, sillä RFID-tunnistus hoitaa ilmoittautumisen automaattisesti. Kahvitauolla Jarmon erityisruokavalio otetaan huomioon ja hänet ohjataan automaattisesti siihen pöytään, jossa ovat tarjolla gluteenittomat korvapuustit. Kotiin päädyttyään Jarmo heittäytyy sohvalle. Kodin tietojärjestelmä tarjoaa Jarmolle katsottavaksi hänen itsensä määrittelemiä suosikkiohjelmia. Jarmo valitsee uutislähetyksen. Tietojärjestelmä muistuttaa vielä, että Jarmon edellisenä iltana aloittama shakkiottelu on vielä kesken. Jarmo jatkaa peliä ja säätää tietokoneen osaamistasoa hiukan alemmaksi. Jarmo ei halua jäädä tänään kotijärjestelmälle toiseksi. Ennen nukkumaan menoaan hän soittaa vielä isälleen.

Reino 74 v: Viriiliä vanhuutta

Reino, 74 vuotta, herää kotoaan. Poikansa Jarmo soitteli edellisenä iltana ja onnitteli uuden auton hankinnasta. Kaikenlaisia fdri-tai-mitä-lie-nappeja täynnä oleva auto on tehnyt senioriin vaikutuksen. Paljon on muuttunut sitten Reinon ensimmäisen auton, joka oli neuvostoliittolainen Mosse 1950-luvulta. Ovet avautuvat, ajo-ohjeita on tarjolla ja peruutustutka estää kolhut pysäköidessä. Samassa innostuksessa Reino tuli hankkineeksi myös elämänsä ensimmäiset farkkunsa. Niissäkin on kuulemma se sama nappi, joka kertoo ympäristölle käyttäjästään. Reino voi itse päättää, että minkä lukuisista RFID-koodeista hän voi halutessaan ottaa käyttöönsä ja missä laajuudessa. Ympäristöstä ja tilanteesta riippuen. Kaikenlaista se insinööri keksii. Kylpyhuoneessa Reinoa odottaa vaa'an lisäksi myös älykäs lääkelajittelija, dosetti. Pillereitä on monia ja moneen vaivaan. Joitakin pitää ottaa päivittäin, joitain joka toinen päivä. Dosetti muistaa mitä milloinkin vaikka Reino ei muistaisikaan. Reinon vaimolla Kaisalla on oma dosettinsa ja RFID-teknologia pitää huolen siitä, että kumpikin saa omat ja oikeat lääkkeensä ajoissa.

Ruokaostokset terveyden ja tarjousten mukaisesti

Reino nappaa kävelysauvat eteisestä ja lähtee kävellen palvelukeskuksen suuntaan. Ensin on tarjolla fysikaalista hoitoa ja hierontaa. RFID-nappi ohjaa Reinon oikeasta huoneesta toiseen ja lopulta uimahalliin. Hoidot tallentuvat automaattisesti tietojärjestelmään, josta hoitaja voi seuraavalla kerralla nähdä Reino hoitohistorian. Myös lounaan ravintotiedot tallentuvat järjestelmään. Tietojen perusteella järjestelmä rakentaa Reinolle seuraavan viikon ruokalistan ottaen huomioon myös lähikaupan seuraavan viikon tarjoukset.

Iltapäivällä Reino istahtaa oman työpisteensä ääreen kotona ja jatkaa omaelämäkertansa toimittamista. Tekstin lisäksi hän hyödyntää vanhoja sähköisiksi skannattuja valokuvia sekä uudempia valokuvia ja videoita. Hänelle on automaattisesti kertynyt elämänsä varrelta oma henkilölogi, josta hän löytää tärkeitä päivämääriä ja sijaintitietoja. Google Earth -karttaohjelmistosta Reino kaivaa esiin karttoja loma- ja työmatkoiltaan eri puolilta maailmaa. Ehkäpä teoksen voisi jo ensi jouluna jakaa sukulaisille joululahjana. Teoksen päivityskin onnistuu siihen saakka kun vaan eloa riittää.

Illalla Reino katselee kodin tietojärjestelmän hänelle ehdottamaa elokuvaa. Järjestelmä kehottaa myös lähtemään vielä kävelylle, mutta Reino päättää olla oman tiensä kulkija. Tekniikasta on apua, mutta ei sen armoille voi sentään jäädä. Reino kaataa siis itselleen pienen tujauksen konjakkia.

Totta vai tarua?

Edelliset tarinat voisivat olla totta jo tänään. Teknologia on jo olemassa, samoin monenlaiset RFID-tekniikkaan liittyvät sovellukset. Ennakkoluulot ja järjestelmien kalleus pitävät RFID-tekniikan arkikäyttäjien määrät vielä toistaiseksi pieninä. Seuraavat vuodet ja kuukaudet näyttävät kehityksen tarkemman suunnan.

Siru on kuitenkin täällä jo nyt.

(Tahvanainen Markus & Tarkka Kai, Systeemityö 1/2007, 23 - 25).

LIITE 2 Biometristen passien liikkeelle laskeminen

Austria (available since 16 June 2006) Passport costs 69.90€. March 2009 all newly issued passports contain fingerprints. http://english.cri.cn/6966/2009/03/30/2001s469447.htm

Belgium (introduced in October 2004): Passport costs 71€ + local taxes. Passports are valid for 5 years.

Bulgaria (introduced in July 2009; available since 29 March 2010). Passport costs 20€. Passports are valid for 5 years. http://www.novinite.com/view_news.php?id=108362

Czech Republic (available since 1 September 2006) Passport costs 600 CZK. Passports are valid for 10 years.

Cyprus (not yet available)

Denmark (available since 1 August 2006): Passport costs DKK 600. Passports are valid for 10 years. http://www.politi.dk/da/borgerservice/pas/pasprisr/

Estonia (available since 22 May 2007): EEK 450 (€28.76) (valid for 5 years). As of 29 June 2009, all newly issued passports contain fingerprints. http://www.nyc.estemb.org/consular_information/passport

Finland (available since 21 August 2006) €46 (valid for max. 5 years). As of 29 June 2009, all newly issued passports contain fingerprints. http://www.finland.org/Public/default.aspx?contentid=166960&nodeid=35831&culture=en-US

France (available since April 2006): €86 or €89 (depending whether applicant provides photographs), valid for 10 years. As of 16 June 2009, all newly issued passports contain fingerprints. http://vosdroits.service-public.fr/F14929.xhtml

Germany (available since November 2005): ≤23 year old applicants (valid for 6 years) €37.50, >24 years (valid 10 years) €59 Passports issued from 1 November 2007 on include fingerprints. http://www.bmi.bund.de/cln_156/DE/Themen/Sicherheit/PaesseAusweise/eReisepass/eReisepass_node.html

http://bundesrecht.juris.de/pa_g_1986/__5.html

Greece (available since 26 August 2006) €76.40 (valid for 5 years). Since June 2009, passports contain fingerprints. http://www.consilium.europa.eu/prado/EN/3218/docHome.html

Hungary (available since 29 August 2006): 6000 HUF (€24), valid for 5 years, 10000 HUF (€40) valid for 10 years. As of 29 June 2009, all newly issued passports contain fingerprints. http://www.epractice.eu/en/news/292210

http://www.kormanyszovivo.hu/news/show/news_1891

Ireland (available since 16 October 2006): €80, valid for 10 years. Free for people over 65. (Not Signatory to Schengen Acquis, no obligation to fingerprint biometrics). http://foreignaffairs.gov.ie/home/index.aspx?id=25133

Italy (available since 26 October 2006): €42.50,[1] valid for 10 years, plus tax stamps of €40.29 per year (first is mandatory; an unexpired tax stamp is only required when passing through Italian passport control). As of January 2010 newly issued passports contain fingerprints. http://poliziadistato.it/pds/file/files/nuovocosto_Passaporto_Elettronico.pdf

http://www.amblavalletta.esteri.it/Ambasciata_LaValletta/Archivio_News/PASSAPORTOIMPRONTE.htm

Latvia (available since 20 November 2007): An adult passport costs €21.53, valid for 5 years. http://www.pmlp.gov.lv/en/pakalpojumi/passport/questions.html

Lithuania (available since 28 August 2006): LTL 100 (€29). For children up to 16 years old, valid max 5 years. For persons over 16 years old, valid for 10 years. http://www.dokumentai.lt/en/pass.php

Luxembourg (available since 28 August 2006): €30. Valid for 5 years. As of 29 June 2009, all newly issued passports contain fingerprints.

Malta (available since 8 October 2008): €70 for persons over 16 years old, valid for 10 years, €35 for children between 10–16 years (valid for 5 years) and €14 for children under 10 years (valid for 2 years).

Netherlands (available since 28 August 2006): Approximately €11 on top of regular passport (€38.33) cost €49.33. Passports issued from 21 September 2009 include fingerprints. Dutch identity cards are lookalike versions of the holder's page of the passport and contain the same biometric information. http://www.paspoortinformatie.nl/english/Authenticity_features/Model_2006/Introduction

Poland (available since 28 August 2006): 140 PLN (€35) for adults, 70PLN for students, valid 10 years. Passports issued from 29 June 2009 include fingerprints of both index fingers. http://www.eng.pwpw.pl/PressInfoEntry?id=152

Portugal (available since 31 July 2006 - special passport; 28 August 2006 - ordinary passport): €60 for adults (€50 for those who are over 65 years old), valid for 5 years. €40 for children under 12, valid for 2 years. All passports have 32 pages. http://www.pep.pt/index_eng.html

Romania (available since 31 December 2008): 266 RON (€67), valid for 5 years for those over the age of 6, and for 3 years for those under 6. As of 19 Jan 2010, new passport includes both facial images and fingerprints. http://www.rcg.tv/html/eng/about/newsroom/industry_news/biometrics/2010_details_18.jsp

Slovakia (available since 15 January 2008) An adult passport(>13years costs 33.19€ valid for 10 years, while a chip-free child's(5–13 years) version costs 13.27€ valid for 5 years and for children under 5 years 8.29€, but valid only for 2 years.

Slovenia (available since 28 August 2006): €36 for adults, valid for 10 years. €31 for children from 3 to 18 years of age, valid for 5 years. €28 for children up to 3 years of age, valid for 3 years. All passports have 32 pages, a 48-page version is available at a €2 surcharge. As of 29 June 2009, all newly issued passports contain fingerprints. http://www.mnz.gov.si/nc/en/splosno/cns/news/article/12027/6380/

Spain (available since 28 August 2006) at a price of €20. They include fingerprints of both index fingers as of October 2009. (Aged 30 or less a Spanish passport is valid for 5 years, otherwise they remain valid for 10 years).

Sweden (available since October 2005): SEK 400 (valid for 5 years). As of 29 June 2009, all newly issued passports contain fingerprints. http://www.swedavia.se/en/Start-page/Travellers/Travel-planning/Passport-and-Visa/

UK (introduced March 2006): £77.50 for adults and £49 for children under the age of 16. (Not Signatory to Schengen Acquis, no obligation to fingerprint biometrics.) http://www.direct.gov.uk/en/Nl1/Newsroom/DG_179060

Unless otherwise noted, none of the issued biometric passports mentioned above include fingerprints as of 5 May 2010.

Albania

The Albanian biometric passport is available since May 2009, €50 and is valid for 10 years. The microchip contains ten fingerprints, the photo and all the data written on the passport.

Armenia

In April 2010 Armenia will introduce two new ID-documents to replace ordinary passports of Armenian citizens. One of the documents – ID card with electronic chip, will be used locally within the country, and the biometric passport to be used for traveling abroad. Electronic chip of biometric passport will contain digital images of fingerprints and photo of passport holder. http://www.plusworld.org/daily/page1_3156.php

Australia

The Australian biometric passport was introduced in October 2005. The microchip contains the same personal information that is on the color photo page of the ePassport, including a digitized photograph. Airport security has been upgraded to allow Australian ePassport bearers to clear immigration controls more rapidly, and face recognition technology has been installed at immigration gates. http://www.customs.gov.au/webdata/resources/files/03ePassports_June2010.pdf

Bosnia and Herzegovina

Available since 15 October 2009 and costing 20.51€. Valid for 5 years. Produced by Bundesdruckerei. On 1 June 2010 Bosnia and Herzegovina issued its first EAC passport. http://www.setimes.com/cocoon/setimes/xhtml/en_GB/newsbriefs/setimes/newsbriefs/2009/07/16/nb-07

Brazil

Brazil will start issuing ICAO compliant passports in December 2010.

Brunei

The Bruneian biometric passport was introduced on 17 February 2007. It was produced by German printer Giesecke & Devrient (G&D) following the Visa Waiver Program's requirements. The Bruneian ePassport has the same functions as the other biometric passports.

Canada

Canada has recently introduced biometrics in the use of passports with the help of digitized photos. The future passports may contain a chip that holds a picture of the person and personal information such as name and date of birth. In the 2008 Federal Budget, Jim Flaherty, Minister of Finance announced the electronic passport will be introduced in 2011. Passport Canada began a pilot project in 2009 for special and diplomatic passport applicants.

This technology is being used at border crossings that have electronic readers that are able to read the chip in the cards and verify the information present in the card and on the passport. This method aims at increasing efficiency and accuracy of identifying people at the border crossing. CANPASS, developed by Canada Border Services Agency, is currently being used by some major airports that have kiosks set up to take digital pictures of a person's eye as a means of identification. http://www.cbsa.gc.ca/prog/canpass/canpassair-eng.html

Croatia

Available since 1 July 2009 and costing 390 HRK (€53). The chip contains two fingerprints and a digital photo of the holder. Since 18 January 2010 only biometric passports can be obtained at issuing offices inside Croatia. Diplomatic missions and consular offices must implement new issuing system until 28 June 2010.

Dominican Republic

In the Dominican Republic, biometric passports began to be issued in May 2004.

The Dominican Republic is the only country whose passport does not have the biometric symbol on its cover. In Jan 2010, the cost of the passport was 1,250 DOP, about 35-40 USD at that date.

Hong Kong SAR

The Hong Kong Immigration Department has, from 5 February 2007, introduced the electronic Passport (e-Passport) and electronic Document of Identity for Visa Purposes (e-Doc/I) which are compliant with the standard of the International Civil Aviation Organization (ICAO). Digital data including holder's personal data and facial image will be contained in the contactless chip embedded in the back cover of e-Passport and e-Doc/I. Application fees & procedures remains unchanged. The Immigration Department pledges to complete the process of an application within 10 working days. For children under 11 year of age not holding a Hong Kong Permanent Identity Card, the processing time is 19 working days. Existing HKSAR Passports and Documents of Identity for Visa Purposes will remain valid until their expiry. http://www.gov.hk/en/residents/immigration/traveldoc/hksarpassport/index.htm

Iceland

Available since 23 May 2006 and costing ISK 5100 (ISK 1900 for under 18 and over 67).

India

India has recently initiated first phase deployment of Biometric e-Passport for Diplomatic Passport holders in India and abroad. The new passports have been designed indigenously by the Central Passport Organization, the India Security Press and IIT Kanpur. The passport contains a security chip with personal data and digital images. Initially, the new passports will have a 64KB chip with a photograph of passport holder and subsequently include the holder's fingerprint(s). The biometric passport has been tested with passport readers abroad and is noted to have a 4 second response time – less than that of a US Passport (10 seconds). The passport need not be carried in a metal jacket for security reasons as it first needs to be passed through a reader, after which generates access keys to unlock the chip data for reader access. India has also given out a contract to TCS for issuing e-passports through passport seva kendra. India plans to open 77 such centers across the country to issue these passports. On 25 June 2008 Indian Passport Authority issued first e-passport to the President of India, Pratibha Patil. The e-passport is under the first phase of deployment and will be initially restricted to diplomatic passport holders. It is expected to be made

available to ordinary citizens from September 2010 onwards. http://www.ndtv.com/convergence/ndtv/story.aspx?id=NEWEN20080050016&ch=5/16/2008%2011:13:00%20AM http://www.indian-tech-news.com/electronic-chip-enabled-passports-soon-in-india/187/

Iran

On 1 July 2007, the Ministry of Foreign Affairs of Iran announced that the diplomatic biometric passports would be issued on 10 July. In 2008 some 15,000 biometric passport were made available to the frequent travelers. Ordinary and service biometric passports were to be issued on a regular basis to the public beginning in 2009. Ordinary biometric passports cost 450,000IRR (US$50).

Iraq

In April 2009, the Iraqi Ministry of Interior - the general passports directorate revealed new electronic system to issue the new A-series passports in contract with the German SAFE ID Solutions, the new series is a biometric passport available to the public which would cost 25,000 Iraqi dinars or about $20 USD.

Macao SAR

Applications for electronic passports and electronic travel permits have been started and processed since 1 September 2009.

Macedonia

Available since 2 April 2007 and costing 1500 MKD or c. €22.

Malaysia

Malaysia was the first country in the world to issue biometric passports in 1998, after a local company, IRIS Corporation, developed the technology. Malaysia is however not a member of the Visa Waiver Program (VWP) and its biometric passport does not conform to the same standards as the VWP biometric document because the Malaysian biometric passport was issued ahead of the VWP requirement. The difference lies in the storage of fingerprint template instead of fingerprint image in the chip, the rest of the technologies are the same. Also the biometric passport was designed to be read only if the receiving country has the authorization from the Malaysian Immigration Department Malaysia started issuing ICAO compliant passports from February 2010.

Sovereign Military Order of Malta

Since 2005 the SMOM diplomatic and service passports include biometric features and are compliant with ICAO standards. http://www.staatsdruckerei.at/pdf/c_274.pdf?75974

Moldova

The Moldovan biometric passport is available from 1 January 2008. The new Moldovan biometric passport costs approximately 99€ and is not obligatory, as it remains valid along with the existing passports. The passport of the Republic of Moldova with biometric data contains a chip which holds digital information, including the holder's signature, as well as the traditional information. From 2011 the new version of the biometric passport will be obligatory for all Moldovan citizens. http://www.registru.md/pa/

Montenegro

The Montenegrin biometric passport was introduced in 2008. It costs approximately €40.

Morocco

The Moroccan biometric passport was introduced in 2008. In December 2009, early limited trials have been extended, and the biometric passport is available from 25 September 2009 to all Moroccan citizens holders of an electronic identity card. It costs 27€. http://www.passeport.ma/

New Zealand

Introduced in November 2005, like Australia and the USA, New Zealand is using the facial biometric identifier. There are two identifying factors - the small symbol on the front cover indicating that an electronic chip has been embedded in the passport, and the polycarbonate leaf in the front (version 2009) of the book inside which the chip is located.

Nigeria

Nigeria is currently one of the few nations in Africa that issues biometric passports, and has done since 2008.

Norway

Available since 1 October 2005 and costing NOK 450 for adults, or c. €50, NOK 270 for children.

Pakistan

In 2004 Pakistan became one of the first countries in the world to issue biometric passports compliant to ICAO standards.

http://www.nadra.gov.pk/index.php?option=com_content&view=article&id=42&Itemid=92

Philippines

On 11 August 2009, the first biometric passport was released for President Gloria Macapagal-Arroyo. The new e-passport has various security features, including a hidden encoded image; an ultra-thin, holographic laminate; and a tamper-proof electronic microchip costing at around 950 pesos.

http://www.gmanews.tv/story/169542/arroyo-first-to-receive-e-passport-from-dfa

http://www.gmanews.tv/story/169543/frequently-asked-questions-regarding-the-39e-passport39

Russia

Russian biometric passport was introduced in 2006. As of 2010, it costs 2.500 rubles (approx. USD 80), use only printed data and photo (i.e. no optional fingerprint etc.), BAC-crypted Biometric passport issued after 1 March 2010 is valid for 10 years.

http://developers.sun.ru/content/view/384/85/

Serbia

Available since 7 July 2008, and from 16 December 2010 costs 20€ (Aged 3 or less a Serbian passport is valid for 3 years, aged 3 to 14 it is valid for 5 years, otherwise passport remain valid for 10 years.)
http://www.mup.gov.rs/cms_cir/dokumenta.nsf/putne-isprave.h#

Singapore

The Immigation & Checkpoints Authority (ICA) of Singapore introduced the Singapore biometric passport (BioPass) on 15 August 2006. With this, Singapore has met requirements under the US Visa Waiver Program which calls for countries to roll out their biometric passports before 26 October 2006.
http://www.mindef.gov.sg/imindef/news_and_events/nr/2006/jul/25jul06_nr2.html

Somalia

The new "e-passport" of Somalia was introduced and approved by the nation's Transitional Federal Government on 10 October 2006. It costs $100 USD to apply for Somalis living inside of Somalia, and $150 USD for Somalis living abroad. Somalia is now the first country on the African continent to have introduced the "e-passport".
http://english.peopledaily.com.cn/200702/09/print20070209_348606.html
http://www.garoweonline.com/artman2/publish/Somalia_27/Somalia_Government_lowers_passport_fee.shtml

South Korea

South Korea now issues biometric passports to its citizens as of 2007.

Sudan

The Republic of the Sudan started issuing electronic passports to citizens in May 2009. The new electronic passport will be issued in three categories. The citizen's passport (ordinary passport) will be issued to ordinary citizens and will contain 48 pages. Business men/women who need to travel often will have a commercial passport that will contain 64 pages. Smaller passports that contain 32 pages only will be issued to children. The microprocessor chip will contain the holder's information in addition to fingerprints. Cost to obtain a new passport will be SDG 250 aprox. 100$, 200 for students and 100 for kids. and the validity of the citizen's passport will be 5 years, and 7 years for the commercial passport.

Switzerland

The Swiss biometric passport has been available since 4 September 2006. Since 1 March 2010, all issued passports are biometric, containing a photograph and two fingerprints recorded electronically. The cost is fixed to CHF 140.00 adult CHF 60.00 for children (-18 years old).
http://www.schweizerpass.admin.ch/pass/de/home/ausweise/pass_10.html
http://www.schweizerpass.admin.ch/pass/de/home/ausweise/pass_10/gebuehr_und_gueltigkeit.html

Republic of China (Taiwan)

Available since 29 December 2008 and costing NT$1,600.

Tajikistan

Biometric passports will be issued in Tajikistan from 1 February 2010. On 27 August 2009, Tajik Ministry of Foreign Affairs and German Muhlbauer signed a contract on purchase of blank biometric passports and appropriate equipment for Tajikistan.
http://www.asiaplus.tj/en/news/198/58564.html

Thailand

The Ministry of Foreign Affairs of Thailand introduced the first biometric passport for

Diplomats and Government officials on 26 May 2005. From 1 June 2005, a limited quantity of 100 passports a day was issued for Thai citizens, however, on 1 August 2005 a full operational service was installed and Thailand became the first country in Asia to issue an ICAO compliant biometric passport.

Turkey

Turkish passports which are compatible with European Union standards have been available since 1 June 2010. Colours of the new biometric passports have also be changed. Accordingly, regular passports; claret red, special passports; bottle green and diplomatic passports wrap black colours. Most recently Turkish Minister of the State announced that the government is printing the new passports at government minting office since the private contractor failed to deliver. Another issue troubling Turks who wish to obtain a passport is the astronomical cost. 360 TL (approximately US$ 230) for a passport valid for 10 years. http://www.epasaport.gov.tr/

Turkmenistan

Turkmenistan became the first country in ex-USSR, in mid-Asia region to issue an ICAO compliant biometric passport. Passport is available since 10 July 2008. http://www.turkmenistan.ru/?page_id=3&lang_id=en&elem_id=13207&type=event

United States

The U.S. version of the biometric passport (sometimes referred to as an electronic passport) has descriptive data and a digitized passport photo on its contactless chips, and does not have fingerprint information placed onto the contactless chip. However, the chip is large enough (64 kilobytes) for inclusion of biometric identifiers. The U.S. Department of State now issues biometric passports only. Non-biometric passports are valid until their expiration dates. Although a system able to perform a facial-recognition match between the bearer and his or her image stored on the contactless chip is desired, it is unclear when such a system will be deployed by the U.S. Department of Homeland Security at its ports of entry. A high level of security became a priority for the United States after the attacks of 11 September 2001. High security required cracking down on counterfeit passports. In October 2004, the production stages of this high-tech passport commenced as theU.S. Government Printing Office (GPO) issued awards to the top bidders of the program. The awards totaled to roughly $1,000,000 for startup, development, and testing. The driving force of the initiative is the U.S. Enhanced Border Security and Visa Entry Reform Act of 2002 (also known as the "Border Security Act"), which states that such smartcard Identity cards will be able to replace visas. As for foreigners traveling to the U.S., if they wish to enter U.S. visa-free under the Visa Waiver Program (VWP), they are now required to possess machine-readable passports that comply with international standards. Additionally, for travelers holding a valid passport issued on or after 26 October 2006, such a passport must be a biometric passport if used to enter the U.S. visa-free under the VWP. http://travel.state.gov/passport/passport_2498.html

Venezuela

Issued after July 2007, RFID chip has photo and fingerprints.